

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	1	(wifi or wi-fi) same (detector or finder or locator)	EPO; JPO; IBM_TDB	OR	OFF	2005/05/25 14:17
L2	371	(wireless) same (detector or finder or locator)	EPO; JPO; IBM_TDB	OR	OFF	2005/05/25 14:22
L3	16	(builtin or built-in or integrated or enclosed) and 2	EPO; JPO; IBM_TDB	OR	OFF	2005/05/25 14:18
L4	8	(power or powered) and off and 2	EPO; JPO; IBM_TDB	OR	OFF	2005/05/25 14:22

Internet google
I.P. com

wifi
wireless

Integrated
builtin

detector
locator
finder

IP.com
PriorArtDatabase

May 25, 2005

USPTO

Secure

Search

Full Text

Concept

Document ID

Recent Disclosures

Publish

Publish Disclosure

My IP.com

Manage Account

Prior Purchases

Prior Disclosures

Events

Main Page

Support

Logout

Fingerprint Lookup

Lookup

Displaying records #1 through 10 out of 500
(search stopped at 500 hits)

Result # 1 Relevance:

**PREVIEW**
this document**Wireless aerials for devices**

2004-02-25

IPCOM000022110D

English

A wireless aerial for a device like a radio or mobile phone that a to be placed remotely away from the device so that it can be lo area of optimal signal strength away from the device itself. The then be located in an area with a poor ...

Result # 2 Relevance:

**PREVIEW**
this document**Customer Premises Equipment Providing Wireless Access to Consolidated Broadband Services**

1999-12-01

IPCOM000014356D

English

Disclosed is equipment that connects wireless devices on the cu premises to a broadband network using standard wireless proto preferred embodiment uses the wireless protocols defined by th (TM) Special Interest Group; see www.bluetooth.com for ...

Result # 3 Relevance:

**PREVIEW**
this document**Location Trigger Facility for Personal Communicati on a Wireless Network**

2003-07-24

IPCOM000018575D

English

The present idea relates to a location trigger facility for persona communication devices on a wireless network. In most cellular telecommunication systems the mobile devices is self-locating, can pin-point it's location more precisely and more easily ...

Result # 4 Relevance:

**PREVIEW**
this document**Portable Wireless Network Signal Detector**

2004-09-24

IPCOM000031424D

English

Portable Wireless Network Signal Detectors

Result # 5 Relevance:

**PREVIEW**
this document**Method for environment-driven mobile devices**

08-Nov-2001

IPCOM000005817D

English

Disclosed is a method for environment-driven mobile devices. B improved functionality for existing small mobile devices (such a digital assistants).

Result # 6 Relevance:

**PREVIEW**
this document**LBALC: Location Based Altimeter and Location Calil**

2003-07-01

IPCOM000016445D

English

Altimeter and positioning systems can be found on a variety of such as watches, GPS devices or mobile phones. These systems the altimeter, need to be recalibrated regularly to deliver good Additionally, weather information like ...

Result # 7 Relevance: **PREVIEW**
this document**Wireless/Portable Internet Data Center Facility**

2001-11-01

IPCOM000015291D

English

This invention disclosure, the Wireless/Portable Internet Data Center Facility, addresses a concept for a (portable) wireless Internet Data Center. The wireless IDC is focused on managing high volumes of wireless, IP traffic anywhere in the world. By virtue of ...

Result # 8 Relevance: **PREVIEW**
this document**Method and System for Automated Personal Preference Adjustments for Traveling User**

2002-11-19

IPCOM000010303D

English

Disclosed is a method and system for storing personal preferences, preferred settings for an automobile driver (including seat adjustments, ventilation and so on) on a personal, portable device. A person carries this device to a foreign ...

Result # 9 Relevance: **PREVIEW**
this document**Method and Apparatus for Emergency Mobile Location**

2003-02-11

IPCOM000011043D

English

This paper describes an emergency mobile location method and uses the unique cellular coding information of an emergency mobile location device, which assists a subscriber in locating the subscriber's position. This paper ...

Result # 10 Relevance: **PREVIEW**
this document**PERSONAL EMERGENCY LOCATOR**

2000-12-25

IPCOM000014592D

English

The system to be disclosed is a method of using the Differential Positioning System (DGPS) in combination with a wireless communication system to report the accurate location of an individual in an emergency situation. The Global Positioning System (GPS) was ...

Displaying page 1 of 50 < BACK | [NEXT](#) >

Search query: wireless finder

[New search](#) | [Modify this search](#)

Some of the search results on this page contain characters not found in English/Western European fonts. These results may not display properly if you have fonts installed which support that language.

All instances of information containing these characters are marked with a small 'v' shown to the left.

Do not warn me about language/font

Copyright © 2005 IP.com, Inc. All rights reserved. |

Portable Wireless Network Signal Detector

Mobile workers may not know where wireless networks are available to them, because they are invisible and people often do not publish their existence. Sometimes people have wireless LANs in their homes or businesses that are not secured, and they wouldn't mind if someone else were to "piggyback" on their network. It would be nice to be able to take advantage of these networks when they're available, or to be able to quickly find an area with good wireless reception. (This idea could apply to other types of wireless connections, like Bluetooth, but I'll use an 802.11b network as my example.)

You can currently find a wireless network by inserting a wireless adapter card into your laptop, powering on your laptop, and using its "site survey" function to find an access point. Recently a few keychain-sized wireless network detectors have come onto the market. On those, you press a button and a set of LEDs lights up to indicate whether you are in range of a wireless network. Using this, you can easily walk around until you find a signal, and set up your wireless network client (whether it be a laptop, or soon, a WiFi phone) in that area.

Another implementation that is workable and inexpensive is to make a docking station for someone's existing wireless PCI card. The docking station would have a battery to power the wireless card, and it would use the card's antenna to pick up and interpret signals. The docking station would have very simple "site survey" software, and it would light up and/or beep to indicate when a wireless network connection is available. The detector could have different indicators for encrypted networks and non-encrypted networks. You could use the encrypted network connection if you know the passcode, and you were just using the detector to find a location with good reception. You could use the non-encrypted network connection if you were looking to connect to any wireless LAN that might be in the area, and you don't have a passcode. The first advantage of this implementation is that you only have to buy the docking station, which could be designed and manufactured cheaply - the site survey software this requires should be simple enough to put on a computer chip, and all of the transceiver technology is already handled by the PCI card. The second advantage is that it would use your own PCI card to pick up the signals, so you could be sure that when you plug the card into your laptop you would get the same or better reception as the docking station.

An extension of the docking station implementation is that you can program it to check certain encryption keys to see if you can find a particular secured wireless network.

An extension of the keychain-sized all-in-one detector is that it can be made small enough and cheaply enough to embed it into other devices. For example, your USB storage keychain or your cell phone could also detect wireless networks for you.

Another extension of the all-in-one detector is to make an even smaller one that actually works like an RFID chip - it activates only when it's in range of a wireless signal, and it does not continuously draw power while it's on. This would have applications in the sensor area. For example, a small wireless network signal detector could wait until a device moved into a WiFi hotspot, and then turn on the main transmitter of the device and synchronize its data.

There are two possible ways to indicate the wireless signal strength: either set a threshold value and only alert when the signal is at least that strong, or measure the signal strength and display it (for example, by lighting up more LEDs as the signal gets stronger).

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property
Organization
International Bureau



(43) International Publication Date
15 April 2004 (15.04.2004)

PCT

(10) International Publication Number
WO 2004/031488 A1

(51) International Patent Classification⁷: E01F 9/06, 9/00, 9/08

(74) Common Representative: KONINKLIJKE PHILIPS ELECTRONICS N.V.; c/o LESTER, Shannon, 1109 McKay Drive, M/S-41SJ, San Jose, CA 95131 (US).

(21) International Application Number:
PCT/IB2003/004323

(81) Designated States (*national*): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(22) International Filing Date: 2 October 2003 (02.10.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/415,703 2 October 2002 (02.10.2002) US
60/468,923 7 May 2003 (07.05.2003) US

(84) Designated States (*regional*): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

(71) Applicant (*for all designated States except US*): KONINKLIJKE PHILIPS ELECTRONICS N.V. [NL/NL]; Groenewoudseweg 1, NL-5621 BA Eindhoven (NL).

(72) Inventors; and

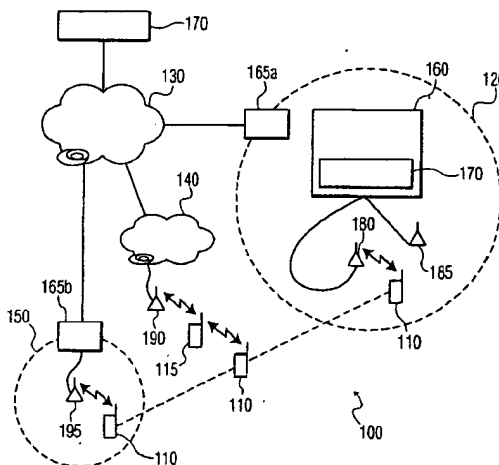
(75) Inventors/Applicants (*for US only*): CHIU, Tom [US/US]; 1109 McKay Drive, M/S-41SJ, San Jose, CA 95131 (US). MELPIGNANO, Diego [US/US]; 1109 McKay Drive, M/S-41SJ, San Jose, CA 95131 (US).

Declaration under Rule 4.17:

— as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii)) for the following designations AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH,

[Continued on next page]

(54) Title: SMART CONNECTION MANAGEMENT OF PORTABLE DEVICES



(57) Abstract: Smart connection management of a portable device (110) may be achieved by storing a customizable profile (245) within the portable device (110) in order to select among a plurality of available connections in accordance with user preferences. The profile (245) may be configured to store configuration parameters (243) for each of the network connection types (e.g., Ethernet, WWAN, WLAN, Wi-Fi, Bluetooth and GPRS) supported by the portable device (110) and user definable selection criteria (247) for selecting between the plurality of network connection types. When the portable device (110) is activated, a connection detector (270) within the portable device (110) detects network connections that are available to the portable device (110). A connection manager (240), coupled to the profile (245) and the connection detector (270), then selects a particular one of the available connections based on the user definable selection criteria (247) and the connection type of each of available network connections, and activates the selected network connection using the stored configuration parameters (243) associated with the connection type of the selected network connection.

WO 2004/031488 A1

HANDTOPS.COM
HANDTOP HEADQUARTERS

[HANDTOP](#)
[REVIEWS](#)
[FORUM](#)
[SITE](#)
[RSS](#)
[SIGN](#)

Wifi Detector

Compare Prices on Wifi Detector.

wifi antennas for 802.11

wifi , wisp equipment for Wireless networking 802.11 B G A

Canary Wifi Finder

Find WiFi hotspots easily. PC World review of 3 that really work.

Wifi detector

Find the best computer deal Compare product reviews

[advertise on handtops.com](#)

[Ads](#)

WiFi Seeker, Finder, Detector roundup

news : Other

Nov 28 2004

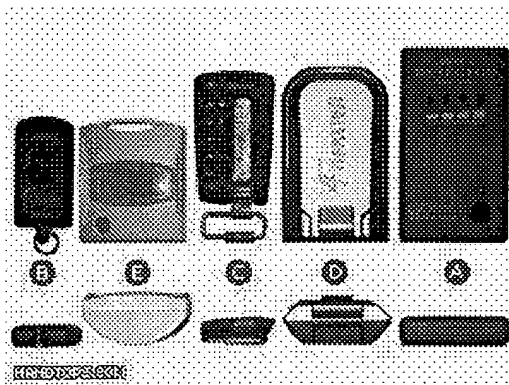
[PLINK](#)
[+STORE](#)

author: captain | 80487 views

[submit news](#)

Finding a handtop or PDA with WiFi isn't such a hard task these days. The wireless networking standard has enjoyed explosive growth in the last few years. Finding a WiFi connection on the other hand, can be an aggravating adventure. If you're not using a WiFi enabled PDA, you either have to turn on your handtop or laptop, or wake it from standby just to check if there's a network in the area. While a WiFi Finder / Seeker won't make a connection out of thin air, it will conveniently tell you whether there is a WiFi network in the area. In this roundup, we look at five reasonably priced hardware WiFi finders.

The players



The following units are reviewed in order of street price:

- (A) Smart ID WiFi Detector - WFS-1
- (B) PCTEL WiFi Seeker
- (C) Kensington WiFi Finder Plus
- (D) Hawking Technologies WiFi Locator - HWL1
- (E) Canary Wireless Digital Hotspotter - HS10

At least one of these tools should be suitable to your needs and wallet. There is a larger size comparison photo and full specification comparison chart at the bottom of this review.

It should be noted that some PDA's do come equipped with great WiFi finders that even show proximity, but this is a roundup of hardware devices whose sole function it is to detect whether a WiFi network exists in the immediate area. All tested devices are available for under \$50USD.



WHAT DO YOU WANT IN YOUR HANDTOP?

[HANDTOP REVIEWS](#)

[Modular PC](#)

QQQ

A fantastic machine

SmartID WiFi Detector (WFS-1)



The good folks at ThinkGeek supplied us with this unit. Judging from online reviews, the WFS-1 appears to currently be one of the most popular WiFi Finders.

Form and design

The design is very simple and fits comfortably on the fingers of your hand while using your thumb to press the button to detect

networks. Sized at 101 x 56 x 14mm (4 x 2.2 x .6") and weighing in at 40g (1.41oz) it's one of the lighter devices we tested. It is also the most no-frills device. The blinking lights look somewhat cheap and the button isn't much better, but everything functions as it should and the look / feel don't actually effect usage.

In use

Detection was moderate and was noticeably weaker than the Hawking Tech HWL1 and Canary WiREless HS10 units but stronger than the PCTEL WiFi Seeker. The specified range is 25-50 feet indoors and 100-200 feet outdoors. For \$24.99USD, the WFS-1 is the cheapest of the lot and has decent range. The simple design puts the focus on functionality and it functions well enough.

PCTEL WiFi Seeker



This device has patented technology to filter out non WiFi signals, so there should be no concerns about false readings from phones or microwaves. To start detecting, you press the large button with your thumb and the LED's will rotate until it spots a connection.

The WiFi Seeker isn't actually made by PCTEL, merely distributed by

them in ODM fashion. The device, called a WiFob, was originally manufactured by Chrysalis Development. Other companies have released the same device in a different body. However, while we would presume them to be entirely similar, we only received and reviewed the PCTEL device and therefore can't comment on whether similar WiFi Seekers function the same or not.

Form and design

OOO

Business user of OOO

VGN-U750P

Wonderful Ultra Portable

VGN-U750P

Great version of U70, but with the flaws of support.

HARDWARE REVIEWS

Iomega Micro Mini 256MB

Great Micro Storage

Buffalo 54 Mbps WiFi USB 2

LAPTOP REVIEWS

Fujitsu P7000

FlyBook

The perfect form factor for a non-gaming

FlyBook

Incredibly small, connectivity powerhouse,

FlyBook

SOFTWARE REVIEWS

Dasher

Dasher is good software, but a keyboard i

Dasher

Though there are many ways to input text unique and fun writing experience.

Tracker

TuneUp Utilities 2004

» Share your thoughts

Designed to be attached to a keychain, PCTEL's WiFi Seeker is extremely light and small -- 57 x 30 x 11mm (2.25 x 1.20 x .43"), 28g (.99oz). The layout is very functional and usable with 4 big and bright LED's. The unit fits comfortably into one's hand.

In use

This device is a breeze to use. Being that it's so small, you are certain to always take it with you, which can't be said for some of the others in this roundup. We often found ourselves taking our keychain out in random areas to see if there was a network available, even if we didn't have a device handy to test that connection. Outdoors it doesn't always have the best success at detecting a WiFi network, but that's not much of a surprise for such a small unit. At times the PCTEL was unable to find anything while the other devices were. Other times, in airports and outside we were able to find networks easily and consistently with the PCTEL.

At only \$29.95USD, the value is great for such a small and functional unit.

Kensington WiFi Finder Plus



Although we weren't able to test the original Kensington WiFi Finder, it had very poor reviews online so we weren't disappointed about its exclusion from our roundup. Kensington's latest WiFi Finder Plus on the other hand could very well save Kensington's reputation in the WiFi finder market. Aside from having good range, it is the only device that can find Bluetooth signals. In addition, there is a

handy flashlight built in.

It may very well be that all or most WiFi finders are capable of filtering out cordless phones, microwaves, cellphones and other devices that operate in the same 2.4GHz spectrum that WiFi does. However, only the Kensington WiFi Finder Plus and PCTEL WiFi Seeker make note of this capability in their literature. Therefore, they may very well be the only ones with this strength.

Form and design

Measuring 89 x 41 x 13mm (3.5 x 1.6 x .5") and weighing only 35g (1.2oz) with a rugged keychain holder, this Finder is roughly the length of the HWL1, but the same thickness as the PCTEL. The keychain holder doesn't appear to be removable. The physical body is slightly rubberized, but only minimally, most likely to provide traction so as to prevent drops, which is a nice touch unique to this device. On the downside, the 5 green WiFi LED's aren't as bright in outdoor situations as the other WiFi Finders. The blue Bluetooth LED is perfectly bright.



ADS

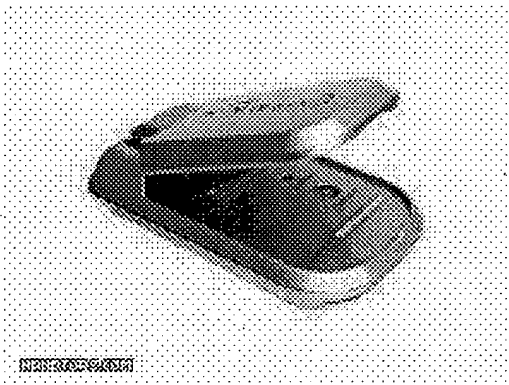
Ads by Google

[WiFi Seeker](#)
[WiFi Hotspots](#)
[WiFi Wireless LAN](#)
[WiFi Sniffer Software](#)

In use

Having heard nothing but bad things about Kensington's earlier attempt at a WiFi Finder, we were pleasantly surprised by this latest model. Detection range was marginally better than the SmartID and PCTEL finders. At times, it even matched performance of Canary's HS10. One concern we had was that it wasn't clear whether this device could detect a bluetooth **and** WiFi network at the same time. There was no note made of this in the included documentation nor the online page. In tests, we were able to find a WiFi network with the HS10 but the Kensington would only find a bluetooth connection. According to Kensington, if both a bluetooth connection and a WiFi connection are present, it will display LED's only for the WiFi connection, but not bluetooth.

One area in which the device lagged behind other models was detection time. Even in situations where other models were able to immediately spot a network, the Kensington consistently took about 3 seconds to do the same. With the others we could be walking along and start detecting immediately, but with the Kensington it felt like we had to stop and wait for it to finish scanning or else we might no longer be in the area of a WiFi network. The accuracy and range appear to be more robust than the SmartID and PCTEL models, but at the price of taking a little more time to detect a signal. The price of \$29.99USD certainly makes it hard to beat for the extra bonuses (bluetooth + flashlight) and range that surpasses the SmartID and PCTEL.

Hawking Technology WiFi Locator (HWL1)

The HWL1 has a high 5.15dB antenna gain, and this large antenna did improve performance noticeably over other models. The extra gain boost allows you to better detect what's in the area. Press the scan button and the five blue onboard LED's light up immediately. The strong antenna coupled with the instant detection allows you to rotate your position or move the device up/down to

detect where the strongest signal might be coming from. This wouldn't be so easy to do with the Kensington or Canary Wireless models which take more time to detect.

Oddly, the included documentation conflicts with the specs sheet on HawkingTech's website. Online, the device is listed as having a range of 300 feet indoors and 1000 feet Line of Sight, while the instruction manual lists it as 610 feet Line of Sight.

Form and design

The HWL1 borrows the clamshell design of today's modern cellphone. But rather than showing you a LCD screen, the portion that flips out is an antenna. Unlike cellphones that you can flip open with one hand, you have to physically open this device with two

hands. Weighing in at 45g (1.59oz) the HWL1 is quite light and its 92 x 56 x 25mm (3.62 x 2.20 x .98") dimensions will feel familiar with cellphone users.

In use

The HWL1 easily had the best range out of all the devices. The cellphone-like design makes for a very inconspicuous looking detection experience. The other WiFi finders may get you some looks with their odd shapes and design.

The only disappointment with the HWL1 is oddly the battery compartment. It took literally 15 attempts to get the device to power on. Putting the battery in isn't the problem, it's getting the two battery connectors to sit correctly when putting the battery compartment back in. After fidgeting about with that for a bit, the device finally worked. Even after being jostled around in a pocket, there weren't any problems with power, so it was just a matter of initial setup. With the lifespan of these batteries being listed as years, this compartment issue shouldn't be a big consideration. The HWL1 will set you back about \$34.99USD, slightly more than other models but you get a much stronger antenna.

Canary Wireless Digital Hotspotter (HS10)



The Digital Hotspotter (HS10) is the only device on the market that not only detects a connection and its strength, but can also tell you whether it is encrypted, what channel it is on and the name of the network. You simply press the button and the device starts scanning and then stops once it finds a network. Press the button again to see if there are other networks on other channels. It can

scan amongst 13 channels.

Form and design

The website for the HS10 doesn't really do the device much justice, it's not clear whether it is the size of a matchbox or the size of a CD case. Fortunately, it's not that large. Measuring a skimpy 64 x 55mm (2.52 x 2.17"), this WiFi Finder is small, but it's quite thick at 27mm (1.06") and a little heavy at 128g (4.52oz). There is a little notch at the top but it's unclear if it's meant to be used for a keychain. While the device is chunky it does feel comfortable in the hand and is actually light to hold.

In use

Out in the field, the HS10 works very well. If any networks are found, it stops scanning and then scrolls the network name (SSID), its strength, whether it is encrypted or open and the channel the network is on. Pressing the button again will

continue scanning.

No other WiFi finder gives you this much information. Knowing whether there are any open networks in the area can save you from powering up / waking up your handtop/laptop, only to find out the network is encrypted. Detection is quick and range is above par, from 300-610 feet.

However, the picture isn't entirely rosy. Given the extensive information provided by the LCD, the HS10 is open to looking less capable. For example, in one room that we tested in, the device wasn't able to detect the wireless router inches away from it. At the same time, it was able to detect other networks in the same building, even ones we weren't aware of before using Netstumbler. Any of the other devices would simply have shown that a connection was available, not telling you whether it recognized your network, your neighbors or both, and that would be the end of it. This would lead you to think that the device was doing its job, when in fact you couldn't really be certain what network it was detecting. The manufacturers explanation for the HS10 not finding the router in the same room is that it only works with 95% of devices. More specifically, Canary Wireless claims that some devices broadcast their beacon frames at a higher than acceptable data rate, which causes the detection conflict. The router in question was a D-Link DI-614+, but the manufacturer mentioned that this problem occurs with a small set of Linksys routers. They did also note that most old and new Linksys and D-Link routers work just fine.

The fact remains that the HS10 found networks that we didn't even know existed before, something that wouldn't really be possible with any of the 4 other units. The range was great and the detection was quick. It may be an issue to some that "only" 95% of routers / access points can be detected. However, this may not be as serious as it sounds. No other company has released information on what percentage of routers / AP's can and cannot be detected with their devices. Thus, the HS10 may in fact be capable of detecting a greater percentage of routers / AP's than any other WiFi finder. The manufacturer reassured me that they put the HS10 through about 10 months of testing both on their own and with major WiFi related device manufacturers. Price of the Canary Wireless Digital Hotspotter is \$49.95USD.

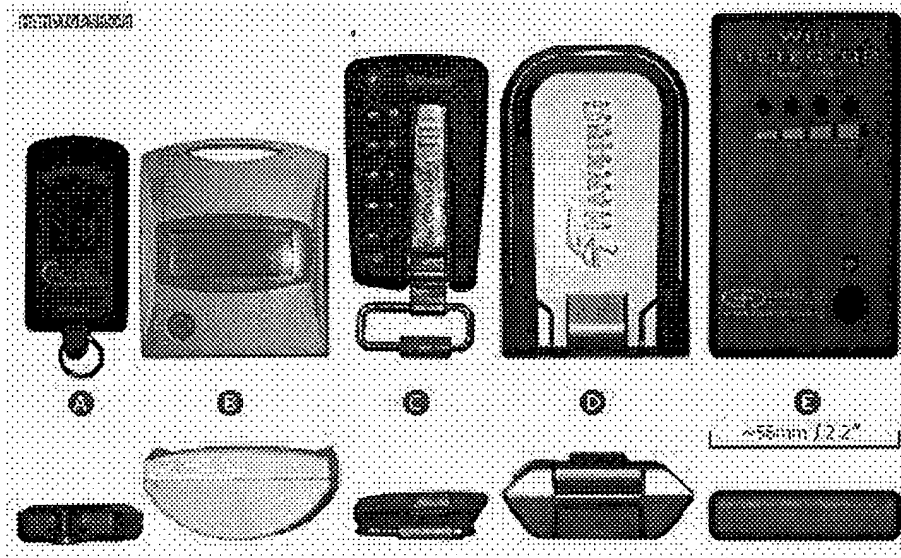
Thoughts

It isn't easy to declare a winner. Even though there are only five devices, most cater to specific needs. The SmartID and PCTEL models are compact, light, and inexpensive, but are weaker at detecting networks. The Canary Wireless and Hawking Tech. models are much stronger and more functional, but much pricier than the other two models. The Kensington does stand out as a winner in the sub \$30USD range with its decent detection range and the bluetooth finder is a bonus. However, it is easily beat out by the Canary HS10 and HWL1 in terms of detection range. Being able to see the network name and whether the network was open or secure are great features unique to the Canary Wireless Digital Hotspotter. For this, some users will certainly be willing to spend the extra coin. In the end, it might save you from having to take out your handtop or PDA, only to find out the network is closed. On the downside, it is double the price of the PCTEL and nearly five times the weight, as well as being much heavier than any of the other devices. The weight is relative however. All of the devices, Canary HS10 included, are light. The Hawking Tech. HWL1 has incredible range and a comfortable form factor, but at the same time, we found it a


























little large for its function. SmartID's WFS-1 is the cheapest of the bunch, but it's a little lumpy, though its range is better than the smaller PCTEL WiFi Seeker.

Prepare to go through a similar back-and-forth. You will have to figure out the top few qualities you are looking for amongst size, range, price and features. We've rounded up the important features in a comparison chart format to help you determine which device(s) might best suit you.

Size Comparison



Spec Comparison Chart

					
Manufacturer	Smart ID	PCTEL	Kensington	Hawking Tech	Canary Wireless
Name	WiFi Detector	WiFi Seeker	WiFi Finder +	WiFi Locator	Digital Hotspotter
Model No.	WFS-1	WiFi S	33086	HWL1	HS10
Specs	802.11b/g	802.11b/g	802.11b/g	802.11b/g	802.11b/g
Bluetooth	-	-	Yes	-	-
Range	25-50, 100-200	up to 300 feet		300-1000 feet	300-610 feet
Accuracy	4 LED's	4 LED's	5 LED's (+1bt)	5 LED's	LCD
Detect WEP	-	-	-	-	Yes
Channel	-	-	-	-	Yes
Detect SID	-	-	-	-	Yes
Flashlight	-	-	Yes	-	-
Battery	2 x AAA	2 x CR2032	2 x CR2016	2 x CR2032	2 x AAA
Dimensions	101 x 56 x 14mm (4 x 2.2 x .6")	57 x 30 x 11mm (2.25 x 1.20 x .43")	89 x 41 x 13mm (3.5 x 1.6 x .5")	92 x 56 x 25mm (3.62 x 2.20 x .98")	64 x 55 x 27mm (2.52 x 2.17 x 1.06")
Weight	40g (1.41oz)	28g (.99oz)	35g (1.2oz)	45g (1.59oz)	128g (4.52oz)
RATINGS					
Size	 80	 95	 90	 75	 82
Range	 77	 75	 80	 95	 92
Features	 75	 75	 85	 75	 95
Price	 95	 92	 92	 85	 75
Price	\$24.99	\$29.95	\$29.99	\$34.99	\$49.95

The future

Ideally, WiFi keychain adapters, such as the Buffalo 802.11b/g USB 2.0 adapter we **reviewed** would have an onboard detector. For the time being, you'll have to bear with adding an extra gadget to your toolbag. Presumably things are going the way of the Canary Wireless HS10 with the ability to see whether networks are open or encrypted. It may not be entirely essential to see the name / channel of a network, but it is useful to know whether it is secure or unencrypted. Perhaps future devices could add an extra LED to denote whether the device has found an open network -- flash red if all found networks are closed, flash green if one is found open. One day perhaps we'll see these devices built into handtops or much smaller keychain-size tools with multi-row LCD displays.

Even with room for improvement and only a small set of WiFi finders on the market, it's great to know that even now there are a healthy set of options to appeal to most.

Official Manufacturer Sites

- Smart ID WiFi Detector - WFS-1 ([official site](#))

- PCTEL WiFi Seeker ([official site](#))
- Kensington WiFi Finder Plus ([official site](#))
- Hawking Technologies WiFi Locator - HWL1 ([official site](#))
- Canary Wireless Digital Hotspotter - HS10 ([official site](#))

RECENT NEWS

New Handtop prototype at WinHEC 2005	 10
More Info on Ruby	 0
Toshiba Libretto U100	 46
New Handtop: Ruby	 13
Toshiba lit-ion battery charges in 60min	 5

COMMENTS

educationk12

11/29/04

Hmmm, I am confused. Will these devices tell you when you can connect to a wifi source. Most WiFi sources are password protected, so it seems to me that these things would be about as useful as a radar detector is in detecting police radar. Seems like you would get a lot of false alarms to wifi that you can't connect to due to password protection.

In NYC you can have a dozen or more wifi signals in one spot. My question is simple:

Do these show you the WiFi signals that are NOT password protected?

If so then it would be worth its weight in gold, but I imagine it is just a device that shows that there is a signal and for someone in NYC that is useless as a wifi signal is everywhere.

Do I have a point, or is there a solution? Seems like the only solution is to turn you computer on and hope for an open connection.

+

educationk12

11/29/04

Which is another reason for EV-DO.

+

captain

11/29/04

Well, the fact is that there is nothing wrong with encrypted connections. If you're in an airport or train, you know that any connection you find will be encrypted, and it's highly unlikely that this connection will be free. Rather, it is an encrypted connection that you can buy time on. That is why it's not true that in all cases you will need to know if a network is an open connection. Of course **ideally** all networks would be open, but all networks cost money, so you're hoping for the impossible.

None of the WiFi finders but the Canary Wireless can tell you if the network is

Secure (encrypted / closed) or Open (unencrypted). Rare these days is the open connection. But that depends on where you live.

In my travels I found some of the lighter options the best because it was obvious that all networks were going to be closed in the airport, but I would be more than happy to buy some time on one.

11 reviews

jkendrick



11/29/04

With a Pocket PC or UPC with WiFi it seems much easier to just whip it out to detect hotspots. I see these dedicated finders more useful for big laptop owners who don't want to pull out the big device unless they know WiFi is present.

jkendrick



11/29/04

Nice review, BTW.

captain

11/29/04

JK, don't forget not everyone owns a PDA ☺ I pointed out in the beginning of the article that PDA's already have this functionality. If you do, great, but not everyone does. I don't, and found some of these finders incredibly useful. You can't compare the price of a \$24.99-\$49 WiFi finder with a few hundred dollar PDA. Plus, you can't exactly put that iPaq on your keychain. ☺

11 reviews

aiiee

11/29/04

Try to buy the Canary Wireless detector. It has been on backorder since the company's inception! Which inception was, according to their website, Nove 9, 2004!



jkendrick



11/29/04

captain, I posted that for the benefits of those owners that have either a PDA or the OQO. They make excellent WiFi finders. Laptop owners can benefit from these finders as I pointed out in my post. I don't believe I compared the prices of the finders with PDAs at all. I was referring to those who already had the mentioned devices.

Did you use the finders with a laptop?

drewzhrodagu11/29/04

You could also use the [WiFiMaps.com AvantGo channel](#) for [WiFiMaps.com](#) to locate hotspots on your PDA or cell phone. We list commercial hotspots, free wireless networks, and other available Wi-Fi networks -- all plotted onto a map of your local area from wardriving data.

+

ajlee11/29/04

Amazingly, 2 hours after posting my last post above, Canary has suddenly gotten their stock in!!!!!!!!!!!!!!

amazing. I didn't know I could cause miracles☺

+

bwolf12/01/04

External antenna jack would be a cool feature to extend range.

+

covact12/02/04

This is the Aricule that I was looking for, thank you. Very Good.

+

register / login

you must be a member to reply or post. [signup](#) or [login](#)

Content and graphics Copyright 2003-2005 handtops.com
All rights reserved. | [Contact](#)

The World's Largest Wi-Fi Business Event **Wi-Fi & VoWiFi!** June 14 - 16, 2005 • Baltimore
Baltimore Convention Center

Enterprise VoIP Planet **The IT Manager's Guide to Voice Over IP**

SPONSORED BY **Evaluate and implement Enterprise VoIP**

www.wi-fiplanet.com/reviews/article.php/3288501

[Back to Article](#)

WiFi Detector
December 12, 2003

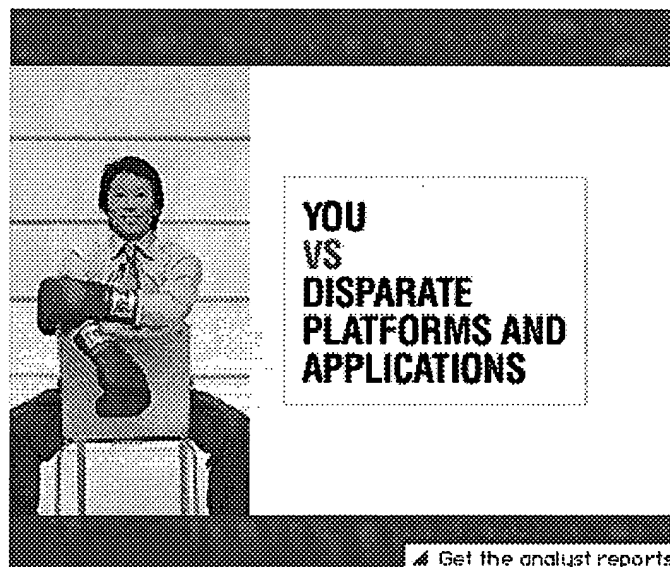
Model: WFS-1

Price: \$28.00 (plus \$10 shipping)

Pros: Geiger counter-like function

Cons: Doesn't tell you if nodes are open

A very specific category of the Wi-Fi product market has eluded review here for a while, that of the inexpensive "Wi-Fi detector." Kensington, famed for locking down laptop PCs, has one but never sent it to us. We've reported on people building them into clothes and handbags, but I had not seen one up close until this week.



Direct from SmartID in Singapore comes the aptly named WiFi Detector, a small rectangular unit about the size of a pack of cigarettes that weighs less about 1.5 ounces. The blister pack it came in calls it the "Ultra Sensative Instant WiFi Detector" and claims it can find a Wi-Fi network in the 2.40-2.48GHz frequency bands (either 802.11b or 11g) within 200 meters outdoors, and 50 meters indoors. It even came with two AAA batteries (the other copper tops: PowerSonic Ultras).

Here's how it works: The back of the unit is really the directional antenna -- point it where you think the RF signal would be. There's a single button on the front of the unit that you push and hold down. A green light indicates if your batteries are up to snuff. A series of four flickering red lights indicate signal strength. No lights mean there are no Wi-Fi radio signals present. Four lights mean you're in the presence of a very strong signal.

Because of the directional nature of the antenna, it can act as a sort of Wi-Fi Geiger counter, leading you in the direction of the nearest access point. The lights usually blink when detecting 802.11 signals, but stay steady for other signals like microwave ovens (they might appear steady in the presence of an extremely strong Wi-Fi signal, as well).

And it works like a charm, exactly as advertised, no more, no less.

In my home, where the access point is in the basement, the signal was strong on the first floor, a little weaker on the second. At the local mall, it definitely knew the local Borders Books and Music had a T-Mobile hotspot inside, and it found a couple of other access points, as well.

That's all well and good, but the Detector doesn't tell you if these networks are open or closed. You don't know if security is turned on, you don't know if you'll be directed to a "walled garden" page at a hotspot, you don't know if the density of users at the access point might prevent you from logging on. All you know is there's an RF signal nearby. In essence, the detector can't give you any indication at all if it's worth whipping out your laptop to try the connection -- you won't know until you actually whip out your laptop and try the connection.

However, if you know there's a hotspot available and you want to position yourself to get the best signal -- all the better to download high-bandwidth movie trailers on your lunch hour -- the Geiger counter aspect of the WiFi Detector lets you sweep an area to see where the best signal is, taking you as close as possible to the access point.

The WFS-1 unit also makes for a quick and dirty security device. I found out that my Wi-Fi signal does indeed travel outside of my house (but someone would have to park in my driveway to get a signal). For locations that don't want any Wi-Fi network at all, the Detector could be the first and cheapest line of defense against rogue access points.

This unit is definitely not as thorough as a true site survey tool or RF detector you can get from companies such as [AirMagnet](#) or [Berkeley Varitronics Systems](#), which can not only detect signals, but analyze them. Even an 802.11-equipped PDA with Netstumbler will tell you more. But, none of the above cost only \$40.

Cut your Wi-Fi Planning, Survey and Reporting time in Half

Ekahau Site Survey 2.1



[Click here for a FREE TRIAL](#)

JupiterWeb networks:

[Internet.com](#)

[EARTHWEB](#)



Search JupiterWeb:

Find

[Jupitermedia Corporation](#) has four divisions:

[JupiterWeb](#), [JupiterResearch](#), [JupiterEvents](#) and [JupiterImages](#)

Copyright 2004 Jupitermedia Corporation All Rights Reserved.
[Legal Notices](#), [Licensing](#), [Reprints](#), & [Permissions](#), [Privacy Policy](#).

[Jupitermedia Corporate Info](#) | [Newsletters](#) | [Tech Jobs](#) | [E-mail Offers](#)

**Wireless Hacks**

By Rob Flickenger

Publisher: **O'Reilly**Pub Date: **September 2003**ISBN: **0-596-00559-8**Pages: **304**Slots: **1.0**

A

A

[Table of Contents](#) | [Index](#) | [Errata](#)

A

Credits

[About the Author](#)[Contributors](#)[Acknowledgments](#)

User name: US Patent & Trademark Office

Book: Wireless Hacks

Section: Chapter 3. Network Monitoring

No part of any chapter or book may be reproduced or transmitted in any form by any means without the prior written permission for reprints and excerpts from the publisher of the book or chapter. Redistribution or other use that violates the fair use privilege under U.S. copyright laws (see 17 USC107) or that otherwise violates these Terms of Service is strictly prohibited. Violators will be prosecuted to the full extent of U.S. Federal and Massachusetts laws.

Hack 20. Find All Available Wireless Networks



Locate all wireless networks in range without installing any additional software.

So, you've got a laptop. You've got a wireless card. The card might even be built into your laptop. You know there are wireless networks in your area. How do you find them? You might even have an external antenna connected to your wireless card, hoping to establish a longer distance connection. How do you find that network a half-mile away?

If you are connected to a wireless network already, you could download a tool like NetStumbler [Hack #21], but this requires a network connection and you don't have one yet.

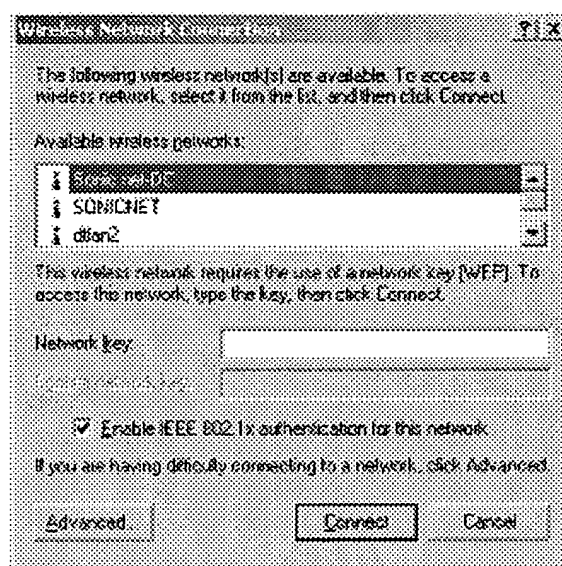
All of the major operating systems have integrated software that allows you to discover wireless networks and obtain some status information about the currently connected network.

Windows XP

If a wireless access point is in range of your wireless card, Windows XP by default will attempt to automatically connect to the access point. It will inform you using a pop up above the task bar, which says, "One or more wireless connections are available."

Clicking on the network icon opens a window titled "Wireless Network Connection," as shown in Figure 3-1.

Figure 3-1. Available networks under Windows XP.

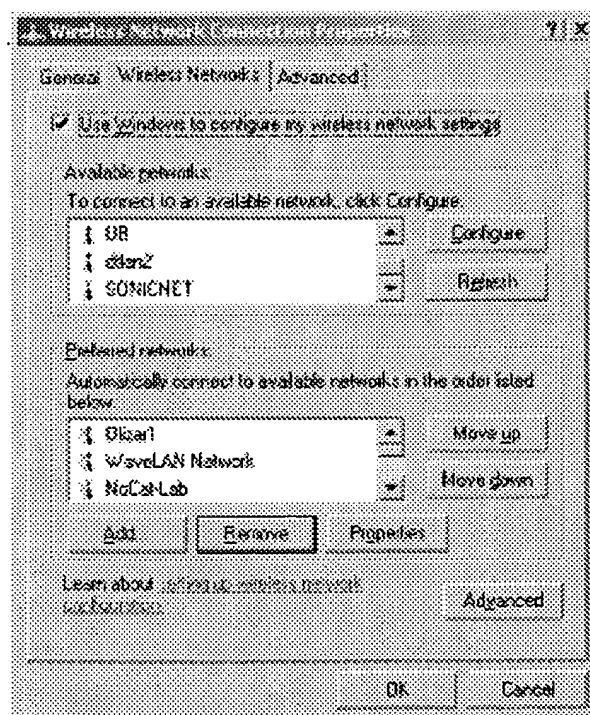


This window lists any wireless networks that are in range of your wireless card. In this example, there are three within range. The window also shows you that the selected wireless network requires the use of a WEP key [Hack #86] in order to join the network.

In order to join this network, you would need to type in the WEP key and then confirm the key by retyping. Once done, you would click on *Connect*. The window will close, and the network icon in the task bar should say "Wireless Network Connection (network name)". The icon also displays the wireless network speed and signal strength.

As shown in Figure 3-1, if you have difficulty connecting to any of the listed networks, you can click on the *Advanced* button, which opens a Wireless Networks window (Figure 3-2).

Figure 3-2. Advanced wireless network options.

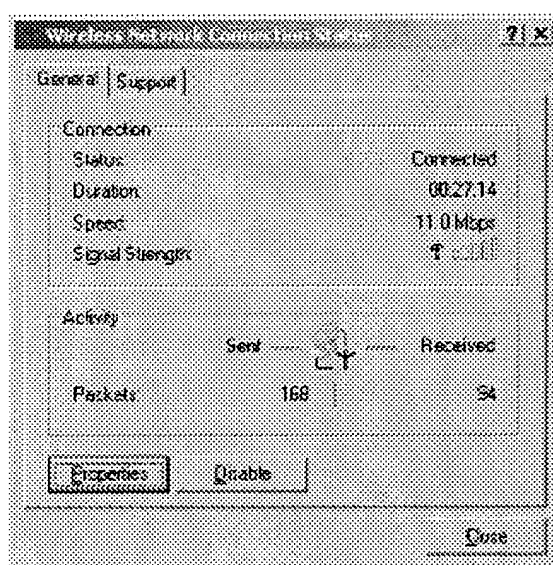


This window again shows the available wireless networks. It also shows a list of "preferred networks" that can be added by the user. This is important to know if your wireless access point does not broadcast the SSID, saving you from repeatedly having to type in the name of the otherwise-invisible network and, indeed, needing to remember its name in the first place. Many access points have the ability to disable SSID broadcast as a security feature (so-called "closed" networks). This means that you need to know the SSID so you can add a preferred network (assuming, of course, that you aren't using a passive monitor like Kismet [Hack #31] or KisMac [Hack #24]).

At the top of this window is the checkbox: *Use Windows to configure my wireless network settings*. If this box is checked, Windows will automatically attempt to connect to any wireless networks listed in your preferred networks. If no preferred networks are available, it will provide you with a list of available wireless networks as shown above.

To get status on the wireless network to which you are currently connected, right-click on the network icon in the task bar and select *Status*. A typical status screen is shown in Figure 3-3.

Figure 3-3. Status details about the connected network.



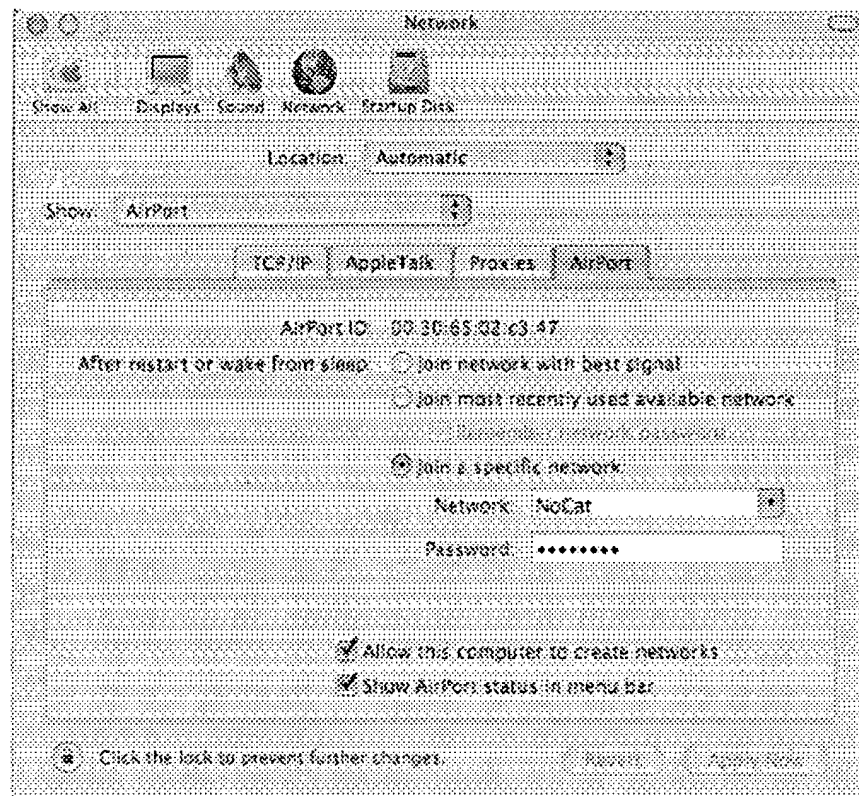
While this gives you some basic connection information, it doesn't show you actual signal strength in dB, which would be very useful for testing wireless connections. You also do not get any information on signal-to-noise ratio. Clicking on the *Support* tab gives you IP addressing information for this wireless card.

Mac OS X

For Apple notebooks with a built-in AirPort card, all wireless configuration is handled through the System Preferences (*System Preferences* → *Network*), as shown in Figure 3-4.

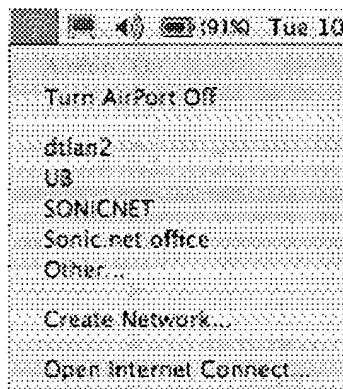
You will likely have two available network cards. Click the *Show* pull-down menu for a choice of adapters, including *Built-in Ethernet* and *AirPort*. Select *AirPort*. To get to the wireless network settings, select the *AirPort* tab.

Figure 3-4. AirPort configuration.



I'll come back to some of this later. Right now, you should be mostly concerned with the *Show AirPort status in menu bar* setting, which should be checked. Once you check this box and close the configuration window, you'll see a new icon in the menu bar (Figure 3-5). The first thing you'll want to do is click the menu bar icon and select the option to turn on the AirPort card.

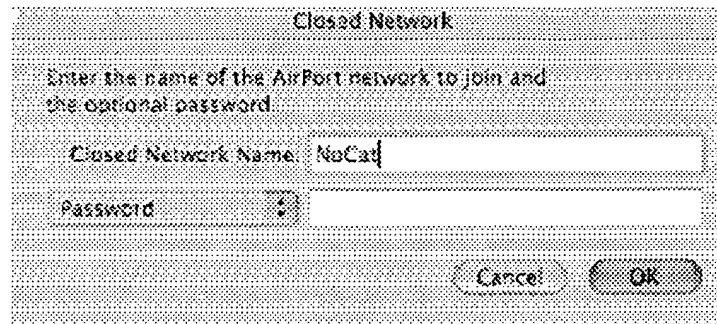
Figure 3-5. AirPort configuration.



Once the AirPort card is on, you'll be able to see a list of available networks; you can select any of these. If a password (WEP key) is required for the selected network, you'll be prompted for it.

To connect to a network that is not listed, click on *Other...*. You will be presented with the *Closed Network* box, as shown in Figure 3-6.

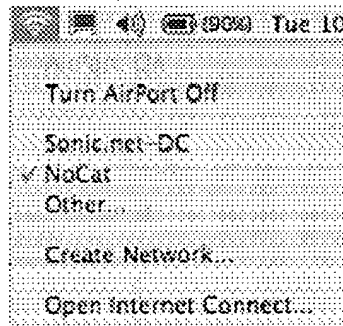
Figure 3-6. Specifying the ESSID for a "closed" network.



Here you can enter the network name (SSID) of the wireless network you want to join and the password (WEP key), if one is required. This is how you can join networks that do not broadcast their SSID.

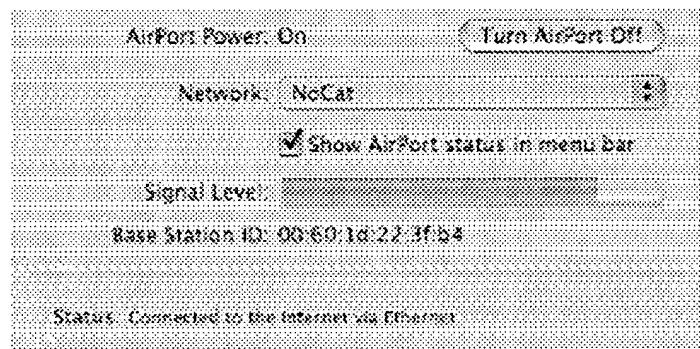
Once you've either selected an available network or entered information for another network not listed, you'll see which network is currently connected by using the AirPort menu bar (Figure 3-7).

Figure 3-7. You can quickly tell which network you are on, and easily choose between all available networks.



The AirPort software offers a signal strength meter, though it is rather limited in its granularity. Click the AirPort icon in the menu bar and select *Internet Connect*; you'll see a window similar to that shown in Figure 3-8.

Figure 3-8. Apple's simple status screen leaves much to the imagination.



Combined with the lack of a connector for external antennas, this severely limits the AirPort wireless card as a useful tool for testing wireless network connections. For more advanced diagnostics, you might want to take a look at MacStumbler [Hack #22].

Linux

Using wireless networking cards in Linux can require a good deal of work, depending on your particular Linux distribution. We're not going to cover that here. This assumes you have PCMCIA support for your wireless card, the Wireless Extensions in your kernel, and the Wireless Tools package installed. Both the Wireless Tools and kernel patches for the Wireless Extension can be found at http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Tools.html. The v.14 Wireless Extensions are included in the 2.4.20 kernel, and v.16 are included in the 2.4.21 kernel.

The Wireless Tools package does come with many distributions. It provides four command-line tools:

iwconfig

Allows you to manipulate the basic wireless parameters

iwlist

Allows you to list addresses, frequencies, bit-rates, and more

iwspy

Allows you to get per node link quality

iwpriv

Allows you to manipulate the Wireless Extensions specific to a driver

iwlist is the tool you need at the command line to show you available wireless networks. To enable scanning, use this:

```
# iwlist wlan0 scanning
```

This gives you detailed information about all detected networks and is supported in the newer versions of the Wireless Extensions/Tools. You'll see output similar to the following:

```
wlan0 Scan completed :
  Cell 01 - Address: 00:02:6F:01:76:31
    ESSID:"NoCat"
    Mode:Master
    Frequency:2.482GHz
    Quality:0/92 Signal level:-50 dBm Noise level:-100 dBm
    Encryption key:off
    Bit Rate:1Mb/s
    Bit Rate:2Mb/s
    Bit Rate:5.5Mb/s
    Bit Rate:11Mb/s
```

If there are multiple access points visible from your machine, you receive detailed information on each one. Once you've found the access point you need to connect to, you can use *iwconfig* to tell your card about it.

Anyone who works with wireless networks in Linux will likely be looking for a more powerful link state monitoring tool. Be sure to take a look at Wavemon [Hack #33] if you need more functionality than the simple command-line tools provide.

—Roger Weeks

URL <http://proquest.safaribooksonline.com/0596005598/wireless-hks-CHP-3-SECT-2>

User name: US Patent & Trademark Office

Book: Wireless Hacks

Section: Chapter 3. Network Monitoring

No part of any chapter or book may be reproduced or transmitted in any form by any means without the prior written permission for reprints and excerpts from the publisher of the book or chapter. Redistribution or other use that violates the fair use privilege under U.S. copyright laws (see 17 USC107) or that otherwise violates these Terms of Service is strictly prohibited. Violators will be prosecuted to the full extent of U.S. Federal and Massachusetts laws.

Hack 21. Network Discovery Using NetStumbler



Find all available wireless networks with this infamous monitoring tool.

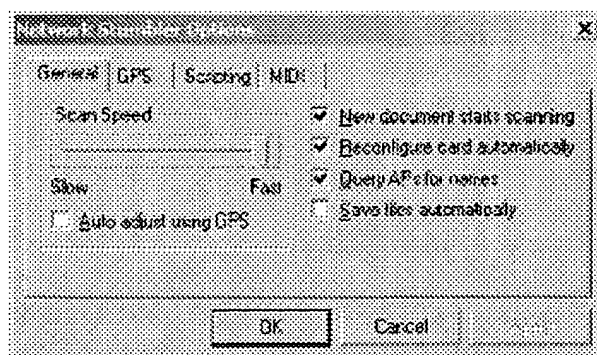
Once you've tried using the wireless client software included with any of the major operating systems, you'll quickly realize the major shortcomings of these utilities. Most tools don't give a detailed measurement of signal strength and won't even indicate when multiple networks are using the same channel.

NetStumbler (<http://www.stumbler.net/>) is an excellent (and free) utility that will give you a great deal of detail about all of the wireless networks in range, including their ESSID, whether they use WEP, the channels they use, and more. As of this writing, the current version is 0.30, and the author is working on Version 0.4. Installation is easy and quick, and for everything that NetStumbler does, the software package is remarkably small.

NetStumbler does not support all wireless network cards. You'll want to check the README before installing to make sure you've got a compatible wireless card. Supported cards include all cards using the Hermes chipset (Lucent/Orinoco/Avaya/Agere/Proxim cards). As of Version 0.30, the software also supports native NDIS 5.1 drivers in Windows XP, allowing it to support Cisco Aironet and some Prism-based cards.

When you launch NetStumbler for the first time, you're going to want to set some options. Click on *View* and select *Options*. You'll see the *Options* dialog as shown in Figure 3-9.

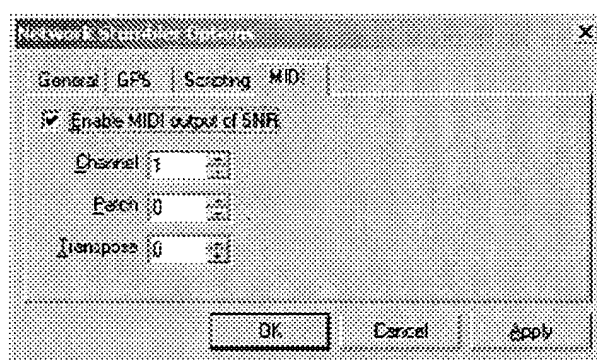
Figure 3-9. NetStumbler Options.



There are a couple of very important options here that you must select to get the best performance out of NetStumbler. You will probably want to set the scan speed to Fast. You'll get more frequent and more accurate updates of wireless networks with this setting. Also, if you are using Windows 2000 or Windows XP, you should definitely check the "Reconfigure card automatically" option. If you don't check this, NetStumbler will find whatever wireless network your card is currently associated with, but no other networks.

One of NetStumbler's coolest features is the ability to give you MIDI feedback for signal strength. This is great for finding the best possible signal between two points, such as when you are trying to align antennas on a long distance shot [Hack #82]. When the signal strength rises, so does the pitch of the tone that NetStumbler plays. This makes tuning an antenna similar to pointing a satellite dish; just move the antenna around until you hear the highest pitch tone. Choose a MIDI channel and patch sounds under the *MIDI* tab of the *Options* screen (Figure 3-10). You'll need a MIDI-capable sound card to use this option.

Figure 3-10. MIDI output options.



With your options properly set, you're ready to discover wireless networks. Assuming your wireless card is installed, NetStumbler will immediately start scanning. If you've got the MIDI option turned on, you'll get a LOT of audio feedback, particularly if you have multiple networks in your area. Figure 3-11 shows a typical NetStumbler session.

Figure 3-11. NetStumbler showing many detected networks.

[illegible]

NetStumbler shows the most active links by color. Green indicates a strong signal, yellow is marginal, and red is almost unusable. Grey means the wireless network is not in reach. The lock symbol shown in many of the link buttons indicates that the network is using WEP.

You can see at a glance all of the wireless networks that NetStumbler has found, along with their signal strength, SNR, and noise. You can also see which vendor chipset the wireless network is using. This can be particularly handy when you are looking for a specific network in a populated area.

To use NetStumbler for fine-tuning a wireless link, start up NetStumbler and make sure that it has found the network on the other end of the point-to-point link. Once it has done so, you'll start hearing the MIDI tones as it reports signal

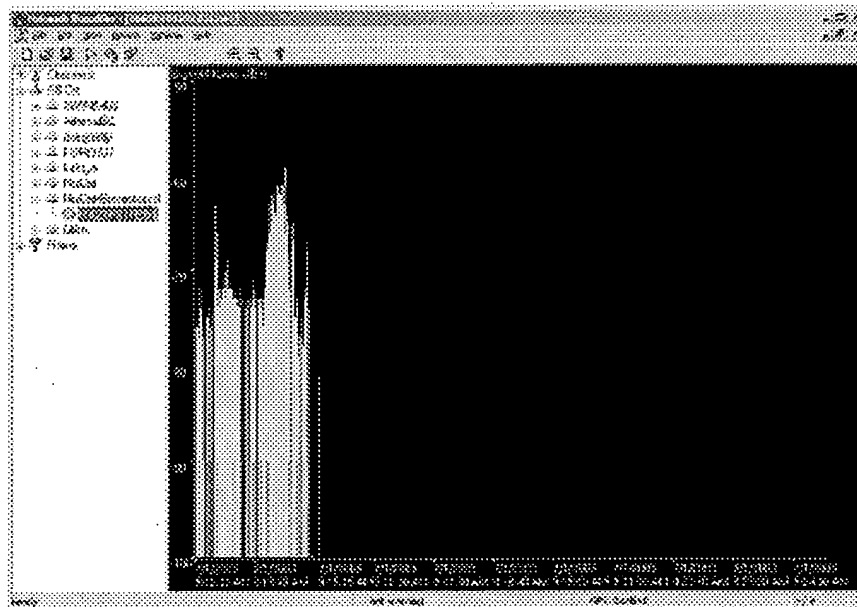
strength. A higher tone indicates better signal strength. Turn up your speaker volume, and then concentrate on pointing the antenna. You'll know it's pointed as accurately it can be when NetStumbler is generating the highest MIDI tone.

A second option to visualize signal strength is available by drilling down through the navigational menus on the lefthand side of the NetStumbler screen. Click on the plus sign next to "SSIDs". You'll see something similar to Figure 3-12 by clicking on the plus sign next to it. You'll see all of the MAC addresses associated with that SSID. Click on the MAC address to see a graphical representation of signal strength to this wireless network. As you can see in Figure 3-13, this is a very handy visual tool. Again, you can use this to tell you when a directional antenna is placed properly. You can also use it in a corporate environment to determine best placement location for an access point.

Figure 3-12. Viewing networks by SSID.

[illegible]

Figure 3-13. The visual meter shows signal strength over time.



NetStumbler will also interface with a GPS system connected to your PC. You can choose your GPS system from a list in the *View* → *Options* dialog. Once you have told NetStumbler about your GPS unit, the main screen not only shows details of the wireless network, but also shows the latitude and longitude of the wireless network.

A note regarding support for wireless cards: as mentioned at the beginning of the back, the author of NetStumbler includes NDIS 5.1 driver support for Cisco and some Prism cards if you are running Windows XP.

In order to make this work, you'll need to click on the *Device* menu. There will be two drivers listed. You must select the driver labeled *NDIS 5.1* in order to make NetStumbler work with Prism or Cisco cards. I've successfully tested this with

the Senao/Engenius 200mW high power cards, and it works well.

NetStumbler is an active network scanner that sends out probe requests and watches for responses to those probes; as such, it won't detect so-called "closed" networks. To accomplish this, you need a passive monitoring tool such as Kismet [Hack #31] or KisMAC [Hack #24]. But for many situations, NetStumbler is a small, powerful tool for detecting and monitoring the majority of wireless networks.

—Roger Weeks

URL <http://proquest.safaribooksonline.com/0596005598/wireless-hks-CHP-3-SECT-3>

User name: US Patent & Trademark Office

Book: Wireless Hacks

Section: Chapter 3. Network Monitoring

No part of any chapter or book may be reproduced or transmitted in any form by any means without the prior written permission for reprints and excerpts from the publisher of the book or chapter. Redistribution or other use that violates the fair use privilege under U.S. copyright laws (see 17 USC107) or that otherwise violates these Terms of Service is strictly prohibited. Violators will be prosecuted to the full extent of U.S. Federal and Massachusetts laws.

Hack 22. Network Detection on Mac OS X



Find out everything you ever wanted to know about the networks available in your area.

If you are simply looking for any available network, you can usually get by with the built-in AirPort client. But if you are building your own network, or troubleshooting someone else's, you need much more detail than the standard clients provide. In particular, knowing which networks are in range and which channels they are using can be invaluable when determining where to put your own equipment. Here are two very easy-to-use survey tools for OS X that give you a far better idea of what's really going on.

MacStumbler

Sharing nothing but a name with the very popular NetStumbler [Hack #21], *MacStumbler* (<http://www.macstumbler.com/>) is probably the most popular network scanner for OS X. It is simple to use, and provides the details that you are most likely interested in: available networks, the channels they use, and their received signal strength. It also displays received noise, whether WEP is enabled, and a bunch of other useful details. See Figure 3-14.

Figure 3-14. MacStumbler's main screen.

MacStumbler GUI									
SSID	MAC	Chan	Signal	Power	Type	Vendor	WEP	WPA	ESSID
100% - 802.11a	00:12:00:00:00:00	1	-60	0	Managed	Apple	No	No	
100% - 802.11a	00:12:00:00:00:00	1	-60	0	Managed	Apple	No	No	
100% - 802.11a	00:12:00:00:00:00	1	-60	0	Managed	Apple	No	No	

Log									
SSID	MAC	Chan	Max	Min	Power	Vendor	WEP	WPA	ESSID
100% - 802.11a	00:12:00:00:00:00	1	-60	0	Managed	Apple	No	No	11:26:00:00:00:00
100% - 802.11a	00:12:00:00:00:00	1	-60	0	Managed	Apple	No	No	11:26:00:00:00:00
100% - 802.11a	00:12:00:00:00:00	1	-60	0	Managed	Apple	No	No	11:26:00:00:00:00

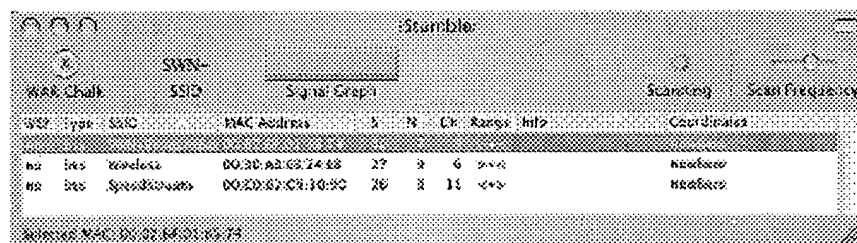
Like many OS X apps, MacStumbler is capable of text-to-speech, so it will even speak the ESSID's of networks that it finds as they appear. Although it is still in beta, I have found MacStumbler to be a very reliable tool. It currently supports network scanning using only the built-in AirPort card.

iStumbler

Another popular network discovery tool is iStumbler (<http://homepage.mac.com/alfwatt/istumbler/>). This tool is even simpler than MacStumbler, in that there is really nothing to configure. Just fire it up and it will find all available networks for you, complete with a real-time signal and noise meter.

As you can see in Figure 3-15, there are plans for GPS support in the next release, but as of v0.6b and at the time of this writing, the Coordinates field is meaningless. Like MacStumbler, iStumbler supports scanning only when using the built-in AirPort card.

Figure 3-15. iStumbler's simple, brushed metal interface.



These tools will both find all available networks quickly, and will keep historical logs if you need to monitor wireless networks over time. If you need to find all available networks in range, either of these tools are ideal.

MacStumbler and iStumbler work by actively sending out probe requests to all available access points. The access points respond to the probes (as they would for any legitimate wireless client), and this information is then collected, sorted, and displayed by the scanners. Unfortunately, neither of these tools will find "closed" networks, since they don't respond to probe requests. This is an unfortunate side effect for people who choose to hide their networks. Since it isn't easy to tell what channel they are using, it is very likely that someone nearby will choose to use the same (or an adjacent) channel for their own network. This causes undesirable interference for everybody. To detect "closed" networks, you need a passive scanner, such as KisMAC [Hack #24] or Kismet [Hack #31].

URL <http://proquest.safaribooksonline.com/0596005598/wireless-hks-CHP-3-SECT-4>

User name: US Patent & Trademark Office

Book: Wireless Hacks

Section: Chapter 3. Network Monitoring

No part of any chapter or book may be reproduced or transmitted in any form by any means without the prior written permission for reprints and excerpts from the publisher of the book or chapter. Redistribution or other use that violates the fair use privilege under U.S. copyright laws (see 17 USC107) or that otherwise violates these Terms of Service is strictly prohibited. Violators will be prosecuted to the full extent of U.S. Federal and Massachusetts laws.

Hack 23. Detecting Networks Using Handheld PCs



Easily monitor wireless networks while walking around.

If you have a handheld PC, you know how convenient it is. What you may not realize is that it makes an excellent wireless testing device. If your handheld has a Compact Flash or PC card slot, you can use a wireless card in these slots.

If you have a Sharp Zaurus or Compaq iPAQ running Linux, then you're in luck. Kismet [Hack #31] runs well on these machines, giving you the most powerful and tiny network monitoring tool there is. When compiling Kismet for a handheld platform, be sure to include the handheld optimizations. See the Kismet documentation for details.

For Pocket PC 3.0 and 2002 users, the author of NetStumbler has written a miniature version just for Pocket PCs: *MiniStumbler*.

MiniStumbler can be downloaded from <http://www.stumbler.net/>. As of this writing, the current version is 0.3.23. MiniStumbler supports Hermes chipset cards only (the Lucent/Orinoco/Agere/Avaya/Proxim strain). There is currently no support for Prism or Cisco cards.

To install MiniStumbler, just copy the proper file for your Pocket PC processor architecture from your host PC over to the Pocket PC. There is no setup routine. Supported processor architectures include ARM, MIPS, and SH3. Check your system documentation if you don't know which one your handheld uses.

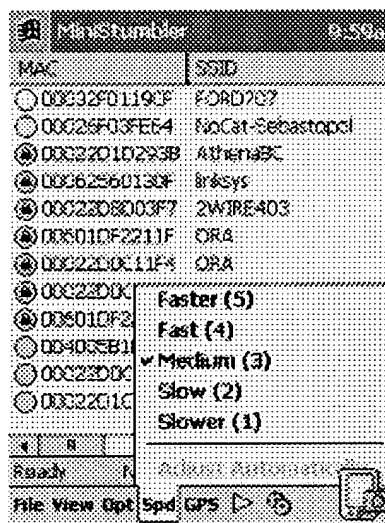
As with NetStumbler [Hack #21], you'll want to set some options the first time you launch it. There are two menus at the bottom that you'll want to check out. The first is Opt, as shown in Figure 3-16. Make sure that *Reconfigure card automatically* and *Get AP Names* are both checked.

Figure 3-16. MiniStumbler's Opt menu.



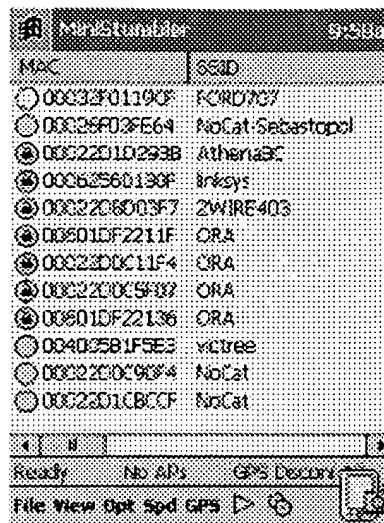
Notably missing from MiniStumbler is MIDI support for audio feedback. However, you can still set the scanning speed, by clicking on the *Spd* menu, as shown in Figure 3-17. Generally, you want to set it to the fastest possible speed.

Figure 3-17. MiniStumbler scanning speed.



With MiniStumbler's options properly configured, you're ready to discover wireless networks. As long as your wireless card is installed, MiniStumbler will immediately start scanning for networks. A typical scanning session looks something like Figure 3-18.

Figure 3-18. MiniStumbler in action.

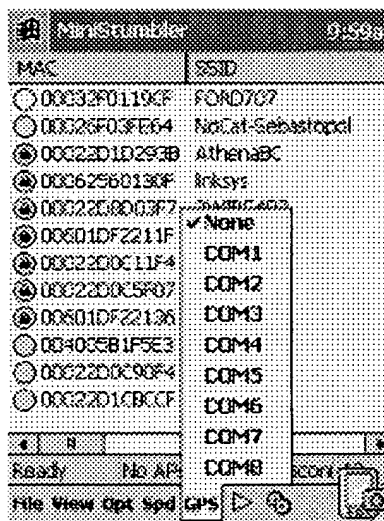


If you've ever used NetStumbler, you should be right at home. The data is displayed in exactly the same way, using the same color scheme for the networks it has detected (green, yellow, or red to indicate signal strength, grey for networks out of range, and a tiny lock icon for networks using WEP). If you need to pause the scanning process, simply click on the green triangle in the bottom menu.

While the tiny screen on a Pocket PC is wonderfully portable, it makes viewing large amounts of data sometimes painful. In order to see all of the data in MiniStumbler, you have to scroll to the right. This includes signal strength, SNR, and noise levels.

MiniStumbler does not support any of the visualization views in NetStumbler, so you can't get a graph of wireless signal over time. However, there is support for location logging using a GPS. Click on the *GPS* menu (Figure 3-19) and select the COM port attached to your GPS. MiniStumbler will then show latitude and longitude locations for all of your wireless networks as it finds them.

Figure 3-19. Select the port to which your GPS is attached.



Obviously, a GPS can only effectively be used for outdoor network detection. But the extreme portability of Pocket PCs make them ideal for performing informal site surveys, checking for unauthorized access points, or establishing the

coverage area of your wireless network. MiniStumbler may be missing many of the handy features of NetStumbler and Kismet, but it is simple to use and far better than the system client for finding networks.

—Roger Weeks

URL <http://proquest.safaribooksonline.com/0596005598/wireless-hks-CHP-3-SECT-5>

File 275:Gale Group Computer DB(TM) 1983-2005/May 25
 (c) 2005 The Gale Group
 File 621:Gale Group New Prod.Annou.(R) 1985-2005/May 25
 (c) 2005 The Gale Group
 File 636:Gale Group Newsletter DB(TM) 1987-2005/May 25
 (c) 2005 The Gale Group
 File 16:Gale Group PROMT(R) 1990-2005/May 24
 (c) 2005 The Gale Group
 File 160:Gale Group PROMT(R) 1972-1989
 (c) 1999 The Gale Group
 File 148:Gale Group Trade & Industry DB 1976-2005/May 25
 (c)2005 The Gale Group
 File 624:McGraw-Hill Publications 1985-2005/May 25
 (c) 2005 McGraw-Hill Co. Inc
 File 15:ABI/Inform(R) 1971-2005/May 25
 (c) 2005 ProQuest Info&Learning
 File 647:CMP Computer Fulltext 1988-2005/May W1
 (c) 2005 CMP Media, LLC
 File 674:Computer News Fulltext 1989-2005/May W3
 (c) 2005 IDG Communications
 File 696:DIALOG Telecom. Newsletters 1995-2005/May 24
 (c) 2005 The Dialog Corp.
 File 369:New Scientist 1994-2005/Apr W2
 (c) 2005 Reed Business Information Ltd.
 File 810:Business Wire 1986-1999/Feb 28
 (c) 1999 Business Wire
 File 813:PR Newswire 1987-1999/Apr 30
 (c) 1999 PR Newswire Association Inc
 File 610:Business Wire 1999-2005/May 25
 (c) 2005 Business Wire.
 File 613:PR Newswire 1999-2005/May 24
 (c) 2005 PR Newswire Association Inc

Set	Items	Description
S1	150046	ACCESS()POINT? ? OR BASE()STATION? ?
S2	6300	S1(7N)(SCAN???? OR DETECT??? OR LOCATE? ? OR LOCATING OR D- ISCOVER??? OR SWEEP??? OR SEARCH???)
S3	3185	S2 NOT PY=2002:2005
S4	2929	S3 NOT PD=20010725:20011231
S5	3902	(ACCESS()POINT? ?)(7N)(SCAN???? OR DETECT??? OR LOCATE? ? - OR LOCATING OR DISCOVER??? OR SWEEP??? OR SEARCH???)
S6	1342	S4 AND S5
S7	737	RD (unique items)
S8	1258	ROGUE()ACCESS()POINT? ?
S9	2	S7 AND S8
S10	2242	(ACCESS()POINT? ?)(6N)(SCAN???? OR DETECT??? OR DISCOVER??? OR SWEEP??? OR SEARCH???)
S11	344	S7 AND S10
S12	9911	WIRELESS()ACCESS()POINT? ?
S13	18	S11 AND S12
S14	17144	WIRELESS(3N)(ACCESS()POINT? ?)
S15	326	S11 NOT S13
S16	19	S14 AND S15

13/9/1 (Item 1 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2005 The Gale Group. All rts. reserv.

02500466 SUPPLIER NUMBER: 74225282 (THIS IS THE FULL TEXT)
WIRELESS NETWORKING -- WIRELESS WORKS -- NetMotion makes the difference in
wireless networks. (Evaluation)
Franklin, Curtis
InternetWeek, 40
May 7, 2001
DOCUMENT TYPE: Evaluation ISSN: 1096-9969 LANGUAGE: English
RECORD TYPE: Fulltext
WORD COUNT: 1059 LINE COUNT: 00087

TEXT:

mobility in the middle NetMotion Mobility intercepts the login traffic from client to server, then manages the traffic from client to server on a pass-through basis.

The idea behind NetMotion Mobility Solution 2.0 is simple: Wireless network users should be able to move from place to place within an organization, receiving network connectivity from the nearest **wireless access point**, without worrying about which subnet the physical access points belong to.

It's the sort of mobility that most wireless users dream about but most wireless network systems have trouble delivering. When NetMotion Mobility is added to the network, though, users can roam across the entire enterprise while administrators secure and manage wireless connections as easily as they deal with traditional cable ports.

The results of NetMotion Mobility's capabilities are impressive. From the user's perspective, there's an "always-on" network connection regardless of where users roam within the organization. The network administrator can set time limits on how long a computer can be out of contact with the network before the network session is shut down for security reasons. So in theory, a user might begin an application in New York, fly to Tokyo, walk into the company's building there and pick up where he or she left off.

The benefits are just as impressive for the administrator, including detailed reports on the activity of wireless devices, enhanced connection security and increased ease for implementing policies and procedures within the network. In short, if you have more than one or two **wireless access points** within your

network and more than a small handful of wireless network users, this is a product that needs to be part of your network infrastructure.

An Artful Dodger

NetMotion Mobility works by playing a bit of a trick on the underlying network. In a normal network login, the client has a direct relationship with the network server. In addition to any application traffic taking place, there are regular "staying-in-touch" communications that let each end know that the other is still in place, still healthy, etc. If the client and server don't have this regular contact for a period of time (variable, but usually ranging from a fraction of a second up to 10 seconds), the server logs the client off the network.

NetMotion Mobility uses a piece of software on the client machine and its NetMotion Mobility Server software to intercept the login traffic from client to server. The NetMotion Mobility Server then logs into the network as the client and manages the traffic from client to server on a pass-through basis. By doing this, NetMotion Mobility can take care of the "Are you there?" traffic whether or not the client is still connected to the network.

If there is traffic back to the client that can't be delivered, NetMotion Mobility stores the traffic until the client re-establishes the link and then picks up as before. The network administrator can set the length of time, from seconds to days, that the client can be out of touch with the network before being logged off. In setting this parameter, the administrator will need to balance the convenience and work habits of

network users against the security issues of having open network logins.

Sniffing Out Clients

We used NetMotion Mobility as part of the infrastructure in the Wireless Networking Lab Test, published in March. After an easy installation process on both a Windows NT server and three Windows 98 laptop clients, NetMotion Mobility was flawless in its main task of providing across-subnet roaming for the clients in tests of various 802.11b networking systems.

We quickly found, though, that NetMotion Mobility provided a number of other important benefits. The first was discovery: We were impressed by the sheer number of **wireless access points** that NetMotion Mobility found on the production network. The software was quite eclectic in its **discovery**, finding **access points** manufactured by every major wireless networking vendor from Apple to Cisco, Enterasys to Symbol. NetMotion Mobility was able to provide connectivity status on the devices attached to each of the access points, making it very easy to get a centralized, overall picture of the wireless network's performance and condition.

It's important to note that we found many **wireless access points** deployed with only rudimentary security in place. If your organization has a proliferation of wireless devices, NetMotion Mobility can provide a centralized way to add connection security and policy enforcement to a diverse, dispersed network. We found that NetMotion Mobility augmented security in ways totally transparent to users, giving administrators the rare opportunity to make both users and managers happier.

Wide-Range Success

In testing NetMotion Mobility with a variety of wireless systems, we found only one instance in which there were any difficulties. Proxim has software that provides some of NetMotion Mobility's features for Proxim systems. When we tested Proxim equipment, we had to take some care in setup to keep the Proxim software from conflicting with NetMotion Mobility. Because none of the other tested systems (including those from Enterasys, Cisco, Intel and Symbol) performed the same functions, there was no special setup required.

The most impressive fact about NetMotion Mobility was simply that it worked, every time, with a variety of systems. It was one of the most quietly impressive pieces of software we've seen in some time. It is, of course, possible to set up a wireless network without NetMotion Mobility. If you're looking at making wireless a key part of your network, though, there's no way that you'll want to leave NetMotion Mobility out of the equation.

Curtis Franklin is managing editor/technology. He can be reached at cfrankli@cmp.com.

WIN SOME, LOSE SOME

Hits

- Provides roaming across subnets
- Works with virtually all 802.11b systems
- Simple setup and administration

Misses

- May conflict with some networking vendor software

THE BOTTOM LINE

NetMotion is key to fulfilling all the promise of wireless networking. It's a no-brainer if your wireless network covers more than a handful of users.

<http://www.internetwk.com/>

Copyright (copyright) 2001 CMP Media LLC

COPYRIGHT 2001 All rights reserved. No part of this information may be reproduced, republished or redistributed without the prior written consent of CMP Media, Inc.

COMPANY NAMES: NetMotion Wireless Inc.--Products

GEOGRAPHIC CODES/NAMES: 1USA United States

DESCRIPTORS: Software single product review; Network software

EVENT CODES/NAMES: 350 Product standards, safety, & recalls

PRODUCT/INDUSTRY NAMES: 7372620 (Network Software)

SIC CODES: 7372 Prepackaged software

NAICS CODES: 51121 Software Publishers
TRADE NAMES: Mobility Solution 2.0 (Network software)--Evaluation
FILE SEGMENT: CD File 275

13/9/3 (Item 3 from file: 275)
DIALOG(R) File 275:Gale Group Computer DB(TM)
(c) 2005 The Gale Group. All rts. reserv.

02484216 SUPPLIER NUMBER: 71557255 (THIS IS THE FULL TEXT)
Cut The Cord -- Wireless networking hits its stride with 802.11b
standard. (Wireless Ethernet) (Hardware Review) (Evaluation)
Franklin, Curtis
InternetWeek, 31
March 12, 2001
DOCUMENT TYPE: Evaluation ISSN: 1096-9969 LANGUAGE: English
RECORD TYPE: Fulltext
WORD COUNT: 5585 LINE COUNT: 00443

TEXT:

The future is wireless, or so we're told. While vendors work out the formula for devices and services that will put wireless clients into every consumer's hands, at least one wireless networking technology has moved out of the early-adopter stage. Wireless Ethernet, defined by the 802.11b standard, is coming into its own as a common technique to connect clients to networks. It is this genuine maturity that new technologies are pushed to achieve. This is the magic place on the product life curve when companies can begin ordering and installing the technology as a solution rather than as an experiment.

We took five separate 802.11b systems to the Review Bunker at the University of Hawaii's Advanced Network Computing Lab to see whether these products truly are as mature as they seem. We wanted to see whether the wireless networking systems would be easy to integrate into an existing network and easy to forget once they were installed. In short, we wanted to find out whether wireless networking systems can replace standard 10Base-T with no performance or management penalties for users and administrators.

Five companies accepted our invitation to this lab test. Cisco, Enterasys Networks, Intel, Proxim and Symbol Technologies brought network access devices, management software and wireless PC cards to the Review Bunker and helped us put the systems through their paces. (See "How We Tested," below.) In the end, we found that there's a lot of good news in wireless networking, along with one little detail that will cause you some trouble.

The good news is that every one of the systems we tested works. All of them performed the basic functions we asked of them, and it's unlikely that choosing any of them would lead to your immediate dismissal from your current position. With all this happiness, what's the bad news? There are significant differences in the way each system works into an overall network architecture, and even more significant differences in the management software provided with each system. You'll have to look at each product and see how it fits in with your current network-as you would any other mature networking product.

The Heart Of Wireless

In 1997, a standards committee of the IEEE defined a wireless networking service with the musical name "802.11." Standard 802.11b uses frequencies in the 2.4-GHz band to transmit data at up to 11 Mbps, though lower rates of 5.5, 2 and 1 Mbps are defined in the standard for situations in which the signal conditions won't allow full network speed. While the signal strength and speed are not solely dependent on distance between access point and client, the two are tied together in such a way that many potential buyers will ask: Will my users notice a performance difference if they are using wireless rather than cabled network access? How far will a wireless system allow users to roam without the need for cables?

The first question is the easier one to answer. We found that in all our tests, the performance of all five wireless systems matched what we

would have expected from a cabled system. This means that the transfer rates we saw were controlled by the application rather than by network transport limitations. It's important to remember that the performance of 802.11b is comparable to that of 10Base-T-if you have users who depend on a 100-Mbps link to move large files around the company, you should leave them attached to the cable.

Distance is a much more difficult issue to pin down. If the question is, "How far will a wireless network stretch?" then the answer is, "It depends." In our tests, we found that some systems lost connectivity with the roaming workstation much more quickly than others. In some situations, systems can hit the limits of usable signal strength within 50 feet of the access point. On the other hand, special-purpose directional antennas can extend the reach of the network to more than 20 miles under ideal conditions. We didn't require our five vendors to demonstrate a 20-mile reach.

In our more limited tests, we found that there were some differences in the range of the systems. As we circled the floor at the lab, three of the systems-Enterasys, Intel and Symbol-demonstrated similar performance. In each case, we walked away from the first access point, down a hallway about 70 feet long. The signal remained strong all the way down the hall and around a corner, until we walked another 20 feet. There, the signal would fade, and we were out of network contact until we rounded the next corner, when the signal from a second access point was raised. The scenario was repeated with the second access point as we continued the circuit around the third corner and back to the beginning.

The two other systems in our test showed a different performance profile. In the case of Proxim, the client lost signal strength long before it diminished with any other system. It was apparent that the antenna Proxim included as standard on the tested units didn't have the radio gain exhibited by other antennas. Cisco's system went in the other direction for performance, never losing touch for more than a couple of seconds as we toured the test circuit. Cisco didn't have magic antennas-it seemed that Cisco's units gracefully stepped down network speed to cope with diminished signal strength without entirely losing contact.

There was no significant difference in the systems' performance in the long-range separation test, which involved a connection dropped for at least 10 minutes to 15 minutes. In every case, the client would lose contact with the access point soon after the elevator doors closed at the lab and re-establish contact when the elevator doors opened on the floor housing the distant access point. There was a bit of good-natured discussion among vendor representatives about precisely when connectivity was lost: If one system lost connectivity as soon as the elevator doors closed while another held connectivity until the elevator descended three or four feet, does that represent a "significant difference"? We decided that it doesn't. If your regular pattern of computer use requires connectivity in an elevator, you should plan to install an access point on the elevator's ceiling-and probably develop a new pattern of computer use.

The Software Side

When we looked for significant differences between the systems, we found them in the management software accompanying each company's solution. Intel and Symbol presented solutions that were nearly identical-not surprising, since there are deep cross-licensing and cooperative development agreements between the two companies. The software accompanying both companies' products shows the influence of Intel's experience in the consumer market. Among all the software we saw, that of Intel and Symbol did the most to help users understand the radio portion of the system, providing Site Survey functions that record signal strength in various locations so that users can plan the final positioning of network components.

Proxim's software bore the influence of a huge installed base of much lower-bandwidth (1 Mbps), earlier-generation equipment. Proxim's greatest strength was the wide variety of filtering and routing provided by the software, so that unnecessary packets aren't sent to clients. It's a set of functions that should be of tremendous interest to the government and institutional users that historically have been heavy Proxim users.

Both Cisco and Enterasys aim their software at the large enterprise user. Enterasys, for example, doesn't do the site survey that Intel and Symbol perform-its assumption is that the professionals on staff already know where equipment should be located. The vendor does provide separate survey tools for use by resellers and installers, and those tools are quite powerful, to the point of helping to generate proposals. Enterasys includes features that make it easy to propagate policies and settings over a large number of access points and clients, easing the load on administrators and managers. Cisco also looks out for the large corporate user, with software that facilitates downloading settings from the policies already established on the enterprise Cisco backbone.

Cisco Aironet 350

Cisco's wireless networking system is designed to extend Cisco's dominance in enterprise networking out through the ether into the radio-frequency realm. To this end, Cisco has presented a solid system with features aimed at enterprise deployment, especially if the enterprise already has Cisco routers on its backbone.

The Aironet access points were installed quickly by the Cisco team, connecting to the ANCL network via an autosensing 10/100Base-T port and drawing power through the Ethernet cable. Since our infrastructure components aren't power-enabled, Cisco provided line power injectors to deliver electricity to the devices. Once we began testing, the Aironet APs worked well, providing the only standout performance on our local-roam test. Virtually all 802.11b access points will step throughput from 11 to 5.5, 2 and finally to 1 Mbps as the signal strength degrades. Cisco was the only system to do so automatically and gracefully, maintaining a link through virtually the entire transit of the local roaming course.

There are a number of ways to configure the software for the Aironet system: An administrator may use Telnet, SNMP, FTP, TFTP, HTTP or a direct serial connection to link with the access point. In addition, the Aironet can automatically configure through receipt of BOOTP or DHCP commands. Setting up the access points was straightforward using parameters we supplied to the Cisco team. Had the ANCL infrastructure been heavily stocked with Cisco backbone components (it wasn't-the lab's infrastructure is a testament to the power of interoperability), setup would have been much easier: Aironet access points can retrieve virtually all their operating parameters from tables established in core Cisco routers. Security keys (either 40-bit or 128-bit) are among the parameters that can be managed either through the core Cisco routers or through management software on the access point. Key management is a crucial issue in wireless security, and Cisco has optimized its management scheme for enterprise applications in which tens to hundreds of access points will be under central control.

Aironet installations can be extended through the use of multifunction or workgroup wireless bridges. The multifunction bridge is designed to link network segments, providing connectivity between access points separated by as much as 18 miles. Workgroup bridges can be configured as either a segment-to-segment bridge, or a combination bridge and access point for up to eight wireless clients.

We were impressed by the combination of excellent roaming performance and enterprise-ready management software. If your enterprise network infrastructure is already heavily populated with Cisco devices, the Aironet system will make propagating policies and keys a painless, nearly invisible process. If not, this is still a solid performer that will provide users wireless connectivity at wired speeds. For the combination of features and performance, the Aironet 350 has earned both InternetWeek Approved and Best of Breed awards in this lab test.

Enterasys RoamAbout

Like the rest of the products we handled in this lab test, the RoamAbout system is competent across a wide range of deployments, but seems particularly suited to a crucial niche. While Cisco seems to target the large enterprise, Proxim the government and institution and Intel/Symbol the remote installation, Enterasys seems to have the management/industrial crossover market squarely in its sights with its design of the RoamAbout. From the decidedly industrial appearance of its access points to case

studies detailing installations on forklifts and robots, Enterasys has designed a system optimized not just to eliminate cables, but to make portability a possibility.

RoamAbout demonstrated local roaming performance that placed it in the mainstream of the tested systems. On the long-distance roaming test, it displayed one interesting characteristic: The client was able to briefly connect to the initial access point when we were outside the ANCL building. We didn't have to walk very far before the signal was lost, but it was a performance differentiator.

Management software was a crucial issue in the test, and Enterasys once again showed an enterprise/industrial bias in the interfaces and functions of the software. While the Enterasys software is not difficult to use for a single access point, it's strong points are facilities for propagating configuration details-especially security keys and filtering rules-across networks of **wireless access points**. Other setup details, such as the "site survey" that measures signal strength and throughput at various locations, are handled by a separate program designed for use by system integrators and commercial installers. The survey software is powerful and complete, but it is not designed with the end user in mind.

The philosophy of the survey tool is evident throughout the RoamAbout software. This is a package designed with a network professional, not a first-time user, in mind. For example, most of the systems we tested will do **access point discovery**-a process of polling through specified IP address ranges to see which devices identify as **wireless access points**. Enterasys software doesn't perform **discovery**-it assumes that the network administrator knows where the devices and their addresses are, and hence will find it easier to simply enter them into the software than to let new pieces of software query the network. While the wireless system can benefit from the features of certain Enterasys switches-drawing, for example, electrical power from the powered-Ethernet ports of some models-it doesn't seem quite so tightly tied to the Enterasys core devices as the Aironet is to a Cisco infrastructure.

RoamAbout systems can be extended through the use of high-gain antennas, with RoamAbout access points acting as both wireless hubs and bridges between segments. Security for the connections is the same as with the other units we tested, either 40- or 128-bit Wired Equivalent Privacy (WEP) security.

Strong hardware performance and software that delivers features friendly to the enterprise network manager earned the RoamAbout system the InternetWeek Approved badge, and let it share the Best of Breed award with Cisco's Aironet.

Intel PRO/Wireless, Symbol Spectrum24 Intel and Symbol each sent teams to the Review Bunker for this lab test. They had adjacent testing slots, and performance that was essentially identical-appropriate results for systems that contained identical hardware and almost identical software. The two companies have signed a number of joint development agreements with the idea of combining Symbol's experience in wireless devices with Intel's expertise in developing and marketing systems for large markets. Both the PRO/Wireless and Spectrum24 seem to bear some fruits of the union.

Both systems performed capably in all our tests, defining the middle of a fairly narrow range of behavior in both device range and speed. The systems come with a pair of "rubber duck" antennas attached to the access points with BNC connectors. The ducks can be replaced with a wide variety of third-party antennas to extend the access points' range, focus the beam to avoid interfering with other devices, or both. Unlike the other systems we tested, the Intel and Symbol access points do not draw their power from the Ethernet connection; they come with a country-specific wall adapter for electrical power.

The management software shipped with the Spectrum24 and PRO/Wireless seeks to make setup and initial administration as simple as possible, even (or perhaps especially) for those with limited wireless networking experience. While there are facilities for propagating security keys and configuration data across large numbers of access points, the emphasis is

clearly on ease of use. Site survey tools are built into the administration software, providing signal strength, throughput, and best channel and address information to an individual making deployment decisions for the system. Once the physical locations are chosen, the software will go out and **discover** other **access points** and wireless clients on the network, to help decide how the topology should be created and which clients should be associated with which **access point**.

The **discovery** process is helpful but, like many helpful tools, should be used carefully. During setup, the Intel team decided to search for other wireless devices on an IP address range that was fairly large. The process involved probing every address within the range for information. When the addresses probed ran through the server farm in the CIS department, TripWire alarms started going off. The IT center's administrator came flying into the lab, convinced that a major hacker attack was under way until we figured that Intel was just trying to see whether the large SP2 data center had lots of hidden wireless network ports. Unless you want to test the efficacy of your server admin's blood pressure medication, we recommend carefully limiting the IP range on discovery probes.

A combination of solid hardware and easy-to-use software earned the InternetWeek Approved badge for both of these systems. Were your deployment plans to call for remote offices to self-install wireless systems, either of these would make a very good choice-as would be the case if you were preparing to install your first wireless system.

Proxim Harmony

Proxim's Harmony was the outlier in our test, and it's important to understand why. First, while there were a couple of areas of performance in which the Harmony system hardware was at the bottom of the list, it was at the bottom of a very narrow range of performance. Next, Proxim has a unique position in the market that it designs systems around, and that position had an impact on our particular testing regimen.

Proxim has a number of different access points in its product stable. The model the vendor brought to our test is a small access point with an interesting antenna configuration. Rather than the rubber duck antennas seen on most of the other products tested, the Harmony used a pair of antennas molded into a plastic bridge that looks like a handle. While unobtrusive-in an office environment, it might blend in with many other features-the antennas didn't seem as effective as the classic ducks in our environment. Proxim sells the same device with a duck-type antenna, so potential customers should be careful talking about particulars when designing an order.

The Harmony software was the only package we looked at that will provide many of the roaming features in NetMotion. Unfortunately, the ability to do this collided with the way some of the production network at the University of Hawaii is set up. Proxim's software uses broadcast packets (UDP) for **access point discovery**-you can't simply tell the software where the **access points** are; it must do the **discovery**. In order for the process to work, UDP must be enabled. Given the open nature of the university's network (there isn't a single firewall point between the network and the Internet), the administrators have disabled UDP for security reasons. While our lab staff and the Proxim team both worked with the university's IT department to find a work-around, time ran out before the problem was resolved. When we discussed the issue with Proxim after the test, the vendor noted that a long-term fix would involve using a DHCP server to provide specific addresses for the access points, and that this would be done in future releases of the software.

The software issue, in particular, seems a result of Proxim's position as a longtime supplier of wireless networking products. There are millions of earlier-generation Proxim systems in the field, many in secure installations at military, government or institutional sites. While Harmony is a system that embodies all current standards, it can't run off and leave its legacy behind. Security and administration with this system are on a par with the other systems in the test-as we stated at the beginning of this article, there were no bad systems brought to the Review Bunker. However, the consequences of Proxim's long history held this system back in

our ratings.

Harmony, looked at as a complete system, earned a B+ in our overall grading chart-a good score, but half a step behind the others. The new version of the software, which uses DHCP rather than UDP, would likely bump Proxim up a half letter, making it a better choice for more customers, and making our job as reviewers that much harder.

HOW WE TESTED

Our testing for the wireless networking systems revolved around two major issues: How well the systems integrated into a total network architecture, and whether they supported seamless client roaming between subnets. Integration into an existing network infrastructure is important because relatively few wireless Ethernet installations will be a "clean sheet of paper" with no regard for the rest of the enterprise. Intersubnet roaming looks at one of the "sexiest" effects of wireless Ethernet-allowing laptop clients to move from location to location without the need to locate RJ-45 jacks or re-establish network identities.

Our "legacy network" was a portion of the production network at the University of Hawaii's Advanced Network Computing Lab (ANCL). Three of its servers, all running Windows NT, were directly involved in our testing. One provided DHCP services for our test network subnets. Another ran Ganymede Software's Chariot 2.1 software to generate three types of traffic: HTTP, POP3 e-mail and FTP (both puts and gets). The third hosted NetMotion software (formerly a WRQ product, now a separate company), which provided the basis for connection maintenance between subnets.

Vendors brought three **wireless access points** and three client network interface cards to the test. The three client NICs went into Compaq Presario notebook computers, each running Windows 98. Each of the clients was designated to receive a different data stream from the Chariot server-one client was designated HTTP, one POP3 and one FTP. Two of the **access points** were located on the floor where ANCL is located. They were on opposite sides of the building, in locations designed to prevent overlap of coverage. The third access point was placed in a building approximately 2,000 feet from the lab. This location was intended to test the system's ability to withstand a lengthy drop in the connection as we walked from one building to the other.

We performed three separate tests, each with the same set of test scripts. The first test, our "control," left the three clients stationary in a location with excellent radio signal strength. This test provided performance data that could be compared to the data from subsequent tests.

In the second test, the HTTP and POP3 clients were left in the same location as in the first test, while the FTP client was carried through the corridor in the ANCL building. While in motion, we observed the client console for both the wireless network system and NetMotion. These clients provided signal strength and connectivity information. After the second test, we verified connectivity information by comparing client data with reports from the NetMotion host console and Chariot.

For the third test, the HTTP and POP3 clients were once again left in position while the FTP client was carried across campus. As in the second test, we monitored network console and NetMotion software, and verified the results at the conclusion of the test.

A CRACKED SPEC

Shortly after we finished testing the systems for this review, word came from the University of California at Berkeley that researchers had managed to compromise the basic security protocol used in wireless networking. The team of Nikita Borisov, Ian Goldberg and David Wagner identified five possible routes through which a security attack can compromise the system. The news, coming as more and more airports, shops and hotels begin to deploy 802.11b networking for guests and customers, has raised questions about the standard's suitability for highly sensitive data.

The Standard

Wired Equivalent Privacy (WEP) is a standard used with 802.11b networking to provide basic security. Since the 802.11 standard doesn't

explicitly address security, WEP has been widely adopted as a mechanism to do two things. First, it protects the network from unauthorized listening or monitoring of the traffic transmitted. Next, it helps prevent unauthorized use of the network.

WEP is an encryption protocol that encodes information packets on transmission, then decrypts them and checks their integrity upon reception. WEP uses a particular algorithm, called RC4 encryption, to encode and decode traffic. RC4 starts with a relatively short encryption key which is then expanded into a nearly infinite stream of keys to accompany the stream of packets. One of the critical factors to good security is making sure that keys aren't reused, since reuse increases the statistical likelihood that someone can figure out the key.

According to the research team, the basic concept of RC4 and other stream ciphers is good, but the way that it's implemented in WEP leaves it open to compromise. In particular, the research focuses on one piece of the implementation, the Initialization Vector (IV) for concern. The IV is the algorithm component that's supposed to keep expanded keys from repeating. Unfortunately, from their point of view, a high-volume access point is mathematically guaranteed to reuse the same key stream at least once a day. When this happens, it's called an IV collision. Further, there are quirks in the implementations of some vendors that would let a lazy administrator force reuse much more often.

Now, it's important to realize that the researchers aren't saying that it's easy to break into the system, or that it's being done on a regular basis. They are saying that it's possible, and the possibility should lead vendors and administrators to consider ways to reduce the possibility. With that in mind, we can look at the five avenues of compromise.

Decrypting Traffic

Decrypting a WEP data stream involves performing a simple logical operation, the exclusive OR (XOR) on the key and the text. If an eavesdropper captures enough traffic using a radio tuned to the proper frequency (this is not a difficult thing to find), then they can wait until an IV collision occurs. If they XOR the two packets using the same IV, they can then begin working backward to figure out the characteristics of the data stream and, ultimately, the contents of the stream.

Injecting Traffic

If an attacker knows the plan text that made up an intercepted message (something fairly easy if the attacker used an external computer to send a message to a system inside the network), she can then work backward to construct the encrypted text by flipping a few bits and performing two XORs. Once this attack is seen to be successful, the attacker can begin sending messages that will be accepted as legitimate by the system-messages that could contain server commands, for instance.

Attacking Both Ends

If the attacker decides to concentrate on the packet headers rather than packet contents, it's possible to begin altering the headers to route packets to systems outside the network, and even choose ports that will allow the packets to move beyond firewalls. If the routing is successfully changed, the wireless system will conveniently decrypt the traffic before forwarding it to the external system-and the unauthorized eyes.

Table-Based Attack

This is a somewhat brute-force method that involves using the relatively small number of IVs to build a decryption table. Once the contents of a single encrypted packet are known, the hacker can work backward and build a table of all the keys possible with a particular IV. Given some time and a single hard disk on a desktop computer, the hacker can build a table of all the keys with all the IVs, at which point any packet can be decoded.

Monitoring

There are a lot of 802.11b devices on the market. Most are designed to ignore packets not addressed to them. The research team was able to modify the drivers for some devices, though, to allow reception and storage of all monitored packets.

Will hackers exploit the possibilities for attacks on 802.11?

Perhaps, but with the knowledge that attacks are possible, administrators can begin reviewing the ways in which wireless systems are deployed, and begin asking questions of vendors, to minimize the potential for damage to their organization.

THE ENVELOPE, PLEASE

It can be tough picking a winner when there are no bad contestants. In this race among competent competitors, though, Cisco and Enterasys Networks rose to the top in terms of offerings for enterprise customers looking to deploy wireless on any significant scale. Cisco's hardware performance edged the rest of the field, while both companies provided software aimed squarely at the needs of large enterprise administrators.

Neither Cisco nor Enterasys will hold your hand through the initial stages of setup, which Intel and Symbol Technologies do quite well. On the other hand, systems from Enterasys and Cisco live up to their enterprise networking heritage by making it easy to deploy and administer thousands of clients and scores-if not hundreds-of access points.

If you're setting up a single wireless subnet, or if your deployment plans include drop-shipping systems to remote office managers who'll perform the installation with telephone support, the Symbol/Intel twins warrant serious consideration. The software shipping with these products makes designing, deploying and managing a small network of wireless devices, or a wireless subnet in a larger network, straightforward and unimposing.

The hardware from both vendors performed well, so the only area in which these systems fall short is in enterprise-class management. It's not that you can't deploy thousands of devices using the software provided by Intel and Symbol-it's just that the job wouldn't be as easy, or the continuing management as smooth, as with the offerings from Cisco and Enterasys.

Proxim was the only system that had any difficulties with our test. The reasons are straightforward.

The hardware that Proxim chose to send us had a built-in pair of antennas that didn't provide the radio signal gain obtained by the antennas on systems from the other vendors. Proxim has a system with replaceable antennas, which should fix the problem, but that version wasn't provided for testing.

On the software side, there were issues because we stipulated that all vendors use the NetMotion software. Proxim's software solution should provide many of NetMotion's subnet roaming features, but it assumes that the total network will allow certain activities that the University of Hawaii's network forbids for security reasons. The solution should work well in a dedicated Proxim environment, but in our tests, the combination worked to the system's disadvantage.

WIN SOME, LOSE SOME

Cisco Aironet 350

Hits

- Strong radio performance
- Enterprise-focused management software

Misses

- Tilted toward Cisco-centric customers

Enterasys RoamAbout

Hits

- Enterprise-focused management software
- Strong lineup of mobile industrial components

Misses

- Site survey tool not part of management software package
- Steep software learning curve

Intel PRO/Wireless

Hits

- Easy-to-use software
- Flexible hardware components

Misses

- Some ease-of-use features may result in users colliding with the

enterprise network

Proxim Harmony

Hits

-Strong packet filtering capability

-Provides cross-subnet roaming as part of basic package

Misses

-Some antenna configurations limited in range

-Roaming requires UDP passing

Symbol Spectrum24

Hits

-Easy-to-use software

-Flexible hardware components

Misses

-Some ease-of-use features may result in users colliding with the

enterprise network

THE BOTTOM LINE

Cisco and Enterasys present the strongest packages for large enterprise customers, though each can have a steep learning curve if the customer isn't already familiar with wireless and the vendor's products. Intel and Symbol shine in ease of use, though some features may make administration of hundreds or thousands of access points more difficult. Proxim is bound by legacy issues with drawbacks that reduce the value of its features.

<http://www.internetwk.com/>

Copyright (copyright) 2001 CMP Media Inc.

COPYRIGHT 2001 All rights reserved. No part of this information may be reproduced, republished or redistributed without the prior written consent of CMP Media, Inc.

COMPANY NAMES: Cisco Systems Inc.--Products; Enterasys Networks--Products; Intel Corp.--Products; Symbol Technologies Inc.--Products

GEOGRAPHIC CODES/NAMES: 1USA United States

DESCRIPTORS: Hardware multiproduct review; Wireless LAN/WAN adapter; Wireless LAN/WAN system

EVENT CODES/NAMES: 350 Product standards, safety, & recalls

PRODUCT/INDUSTRY NAMES: 3662116 (Wireless Local Area Networks)

SIC CODES: 3663 Radio & TV communications equipment

NAICS CODES: 33422 Radio and Television Broadcasting and Wireless Communications Equipment Manufacturing

TICKER SYMBOLS: CSCO; INTC; SBL

TRADE NAMES: Cisco Systems Aironet 350 (Wireless LAN/WAN adapter)--Evaluation; Enterasys Networks RoamAbout (Wireless LAN/WAN system)--Evaluation; Intel PRO/Wireless (Wireless LAN/WAN system)--Evaluation; Symbol Technologies Spectrum 24 (Wireless LAN/WAN system)--Evaluation

FILE SEGMENT: CD File 275

13/9/4 (Item 4 from file: 275)

DIALOG(R) File 275:Gale Group Computer DB(TM)

(c) 2005 The Gale Group. All rts. reserv.

02425395 SUPPLIER NUMBER: 63919411 (THIS IS THE FULL TEXT)

Anatomy of IEEE 802.11b Wireless -- Slice open the standard and see how it turns an 11-Mbps data rate into 6 Mbps of throughput.(Technology Information)

Conover, Joel

Network Computing, 96

August 7, 2000

ISSN: 1046-4468

LANGUAGE: English

RECORD TYPE: Fulltext

WORD COUNT: 2032

LINE COUNT: 00152

TEXT:

Thanks to new and improved silicon technology, lower prices and a high degree of product interoperability, 802.11b high-rate wireless LANs are moving into the enterprise space.

Bit on a Wire

IEEE 802.11b data is encoded using DSSS (direct-sequence spread-spectrum) technology. DSSS works by taking a data stream of zeros and ones and modulating it with a second pattern, the chipping sequence. In 802.11, that sequence is known as the Barker code, which is an 11-bit sequence (10110111000) that has certain mathematical properties making it ideal for modulating radio waves. The basic data stream is exclusive OR'd with the Barker code to generate a series of data objects called chips. Each bit is "encoded" by the 11-bit Barker code, and each group of 11 chips encodes one bit of data.

The wireless radio generates a 2.4-GHz carrier wave (2.4 to 2.483 GHz) and modulates that wave using a variety of techniques. For 1-Mbps transmission, BPSK (Binary Phase Shift Keying) is used (one phase shift for each bit). To accomplish 2-Mbps transmission, QPSK (Quadrature Phase Shift Keying) is used. QPSK uses four rotations (0, 90, 180 and 270 degrees) to encode 2 bits of information in the same space as BPSK encodes 1. The trade-off is that you must increase power or decrease range to maintain signal quality. Because the FCC regulates output power of portable radios to 1 watt EIRP (equivalent isotropically radiated power), range is the only remaining factor that can change. Thus, on 802.11 devices, as you move away from the radio, the radio adapts and uses a less complex (and slower) encoding mechanism to send data.

In 1998, Lucent Technologies and Harris Semiconductor (now owned by Intersil Corp.) jointly proposed to the IEEE a standard called CCK (Complementary Code Keying). To achieve 11 Mbps, the vendors had to change the way they went about encoding the data. Rather than using the Barker code, they used a series of codes called Complementary Sequences. Because there are 64 unique code words that can be used to encode the signal, up to 6 bits can be represented by any one particular code word (instead of the 1 bit represented by a Barker symbol).

The CCK code word is then modulated with the QPSK technology used in 2-Mbps wireless DSSS radios. This allows for an additional 2 bits of information to be encoded in each symbol. Eight chips are sent for each 6 bits, but each symbol encodes 8 bits because of the QPSK modulation. The spectrum math for 1-Mbps transmission works out as 11 megachips per second times 2 MHz (the null-to-null bandwidth of a BPSK signal) equals 22 MHz of spectrum. Likewise, at 2 Mbps, you are modulating 2 bits per symbol with QPSK, 11 megachips per second, and thus have 22 MHz of spectrum. To send 11 Mbps, you'd send 11 million bits per second times 8 chips/8 bits, which equals 11 megachips per second times 2 MHz for QPSK-encoding, yielding 22 MHz of frequency spectrum.

It is much more difficult to discern which of the 64 code words is coming across the airwaves, because of the complex encoding. Furthermore, the radio receiver design is significantly more difficult. In fact, while a 1-Mbps or 2-Mbps radio has one correlator (the device responsible for lining up the various signals bouncing around and turning them into a bitstream), the 11-Mbps radio must have 64 such devices.

Physical Signals

The wireless physical layer is split into two parts, called the PLCP (Physical Layer Convergence Protocol) and the PMD (Physical Medium Dependent) sublayer. The PMD takes care of the wireless encoding explained above. The PLCP presents a common interface for higher-level drivers to write to and provides carrier sense and CCA (Clear Channel Assessment), which is the signal that the MAC (Media Access Control) layer needs so it can determine whether the medium is currently in use (see "IEEE 802.11 PHY Frame Using DSSS," page 96).

The PLCP consists of a 144-bit preamble that is used for synchronization to determine radio gain and to establish CCA. The preamble comprises 128 bits of synchronization (scrambled 1 bits), followed by a 16-bit field consisting of the pattern 1111001110100000. This sequence is used to mark the start of every frame and is called the SFD (Start Frame Delimiter).

The next 48 bits are collectively known as the PLCP header. The header contains four fields: signal, service, length and HEC (header error check). The signal field indicates how fast the payload will be transmitted

(1, 2, 5.5 or 11 Mbps). The service field is reserved for future use. The length field indicates the length of the ensuing payload, and the HEC is a 16-bit CRC of the 48-bit header (for comparison with an Ethernet frame, see "Ethernet PHY Frame" illustration, page 96).

To further complicate the issue (and degrade performance) in a wireless environment, the PLCP is always transmitted at 1 Mbps. Thus, 24 bytes of each packet are sent at 1 Mbps. The PLCP introduces 24 bytes of overhead into each wireless Ethernet packet before we even start talking about where the packet is going. Ethernet introduces only 8 bytes of data. Because the 192-bit header payload is transmitted at 1 Mbps, 802.11b is at best only 85 percent efficient at the physical layer.

It's All a Matter of Timing

The most basic portion of the MAC layer is the ability to sense a quiet time on the network and then choose to transmit. Once the host has determined that the medium has been idle for a minimum time period, known as DIFS (DCF (Distributed Coordination Function) Inter-Frame Spacing), it may transmit a packet. If the medium is busy, the node must wait for a time equal to DIFS, plus a random number of slot times. The time between the end of the DIFS period and the beginning of the next frame is known as the contention window.

Each station listens to the network, and the first station to finish its allocated number of slot times begins transmitting. If any other station hears the first station talk, it stops counting down its back-off timer. When the network is idle again, it resumes the countdown. In addition to the basic back-off algorithm, 802.11 adds a back-off timer that ensures fairness. Each node starts a random back-off timer when waiting for the contention window. This timer ticks down to zero while waiting in the contention window. Each node gets a new random timer when it wants to transmit. This timer isn't reset until the node has transmitted (see "Contention Window," page 97).

Clear To Send?

In "The Hidden-Node Problem" illustration on page 97, workstations A, B and C can all see wireless access point P. Workstations A and B can see one another, and B and C can see one another, but A can't see C. This happens often in real-world wireless environments, where walls and other structures create obscure radio coverage areas.

To handle this situation, an RTS/CTS (request to send/clear to send) is specified as an optional feature of the IEEE 802.11b standard. RTS/CTS solves the hidden-node problem in the following fashion:

When node A wants to transmit some data to node B, it first sends an RTS packet. The RTS packet includes the receiver of the data transmission ensuing and the duration of the whole transmission, including the ACK related to it. Node B hears this request (as do nodes D and E). Node A must use the standard transmission method to obtain access to send the RTS packet. Once the packet is received by the receiving host, that host replies with a CTS message that includes the same duration of the session about to happen. When node B replies with this CTS message, node C (and F and G) hears this response and is made aware of the potential collision, and will hold its data for the appropriate amount of time, preventing a collision. If every node on the network is using RTS/CTS, collisions are guaranteed to occur only while in the contention window. Access points also participate in the RTS/CTS process when necessary.

RTS/CTS adds significant overhead to the wireless 802.11 protocol, especially at small packet sizes. If used, RTS/CTS thresholds must be set on both the access point and the client side.

Power Saving and DTIMs

By default, wireless LANs use CAM (Constant Access Mode) to constantly listen to the network and get the data they need. When power utilization is an issue, however, the workstations and access points can be configured for PAM (Polled Access Mode). With this, the clients on the network wake up on a regular period and listen for a special packet called a TIM (traffic information map) from the access point. In between TIMs, the client shuts off its radio and thus conserves power. All the devices on the network share the same wake-up period, as they must all wake up at exactly the same time to hear the TIM from the access point.

The TIM informs certain clients that they have data waiting at the access point. A client card stays awake when the TIM indicates it has messages buffered at the access point until those messages are transferred, and then the card goes to sleep again. The access point buffers the data for each card until it receives a poll request from the destination station. Once the data is exchanged, the station goes back into power-saving mode until the next TIM is transmitted. In our lab tests, we've found that PAM mode can save power by as much as 1,000 percent, depending on the volume of traffic on your network.

The access point indicates the presence of broadcast traffic with a DTIM (delivery traffic information map) packet. The DTIM timer is always a multiple of the TIM timer and is often adjustable at the access point. Setting this value high cuts down on the amount of time the station must stay awake checking for broadcast traffic. However, a higher DTIM timer means that the radio will stay on longer to receive DTIM traffic when it does come up in the time cycle.

Roaming

In a typical environment, two or more access points will provide signals to a single client. The client is responsible for choosing the most appropriate access point based on the signal strength, network utilization and other factors. When a station determines the existing signal is poor, it begins **scanning** for another **access point**. This can be done by passively listening or by actively probing each channel and waiting for a response.

Once information has been received, the station selects the most appropriate signal and sends an association request to the new access point. If the new access point sends an association response, the client has successfully roamed to a new access point (make, then break behavior).

MAC Layer and Data Payload

In addition to collision avoidance, timing and roaming, the MAC layer is also responsible for identifying the source and destination address of the packet being sent, as well as the data payload and a CRC. The entire payload of the packet, including the MAC header, is transmitted at the rate specified in the PLCP (see "IEEE 802.11 Packet Structure," page 98, and, for comparison, "Ethernet Packet Structure," above).

Send your comments on this article to Joel Conover at jconover@nwc.com.

<http://www.nwc.com/>

Copyright (copyright) 2000 CMP Media Inc.

COPYRIGHT 2000 CMP Media, Inc.

COMPANY NAMES: Lucent Technologies Inc.--Planning; Harris Corp.

Semiconductor Group--Planning

GEOGRAPHIC CODES/NAMES: 1USA United States

DESCRIPTORS: Wireless application protocol; Protocol; Technology development

EVENT CODES/NAMES: 600 Market information - general

PRODUCT/INDUSTRY NAMES: 3674000 (Semiconductor Devices)

SIC CODES: 3674 Semiconductors and related devices

NAICS CODES: 334413 Semiconductor and Related Device Manufacturing

TICKER SYMBOLS: LU; HRS

FILE SEGMENT: CD File 275

13/9/5 (Item 5 from file: 275)

DIALOG(R)File 275:Gale Group Computer DB(TM)

(c) 2005 The Gale Group. All rts. reserv.

02416001 SUPPLIER NUMBER: 63272392 (THIS IS THE FULL TEXT)

Cisco Aironet Beats Rivals-With Ease -- While Cisco's 340 Series rides its friendly features to the top, Lucent Technologies' Orinoco solution nabs our award as the best value in 802.11b networking. (Hardware Review) (Evaluation)

Conover, Joel

Network Computing, 98

July 10, 2000

DOCUMENT TYPE: Evaluation

ISSN: 1046-4468

LANGUAGE: English

RECORD TYPE: Fulltext

WORD COUNT: 4338

LINE COUNT: 00343

TEXT:

Cisco Systems Cisco Aironet 340 Series

Network Computing Editor's Choice

Grade: A-

The Cisco Aironet 340 Series earns our Editor's Choice award because of the wireless hardware's top-notch performance, ease of installation and overall ease of use in our lab tests. Likewise, the Cisco Aironet 340 Series Access Point (AIR-AP342E2C) packs a lot of features and functionality into a very small package. The Cisco access point has features that simplify deployment, and it includes all the functionality an enterprise needs to fine-tune a wireless network. The clear and concise management interface is a dream for both novice wireless users and advanced power users. The interface, which can be accessed via a serial port, telnet or a Web interface, is aware of multiple access points in the network and capable of managing a cluster of **wireless access - point** devices as a managed group. However, Cisco-and the industry in general-has a long, long way to go to make managing an enterprise of wireless devices less of a headache.

The Cisco Aironet 340 Series PC Card (AIR-PCM342) is well-designed; its solid single-piece construction is rugged and durable. The access point-PC Card combo outperformed every vendor's solution by at least 15 percent in raw throughput tests. The 340 Series PC Card has a 5-volt design. Cisco's product sits in the middle of the pack in terms of power consumption. Its power-saving mode delivers excellent throughput, but the unit's 500-milliwatt quiescent power draw drops it to fifth in our power-consumption tests. The 340 Series' strong showing was gained through proprietary (though interoperable) performance extensions. Our ongoing lab tests have shown that Cisco products don't soar nearly as high when non-Cisco PC Cards are used with Cisco access points.

The Aironet family of products seems to be aimed primarily at Wintel PC users; no support for Microsoft Windows CE or Apple Computer Macintosh was available during our tests. In addition, Cisco charges the most for its units, demanding a hefty \$249 per PC Card. The Cisco tax strikes once again. Pricing is an interesting game in this market, however. For example, Lucent Technologies sells its access point for \$1,000 but also requires the purchase of a wireless PC Card to put in the access point. Likewise, Cisco charges additional fees for antenna diversity and encryption, even though these options are "software upgrades." And all this is calculated without discounts the vendor may offer.

Cisco's PCI-based adapter is simply a PC Card mounted on a PCI-based PCMCIA host adapter. Most vendors take this approach, and even those that don't (such as Compaq Computer Corp., with its WL200 11 Mbps Wireless LAN PCI Card) still identify the PCI card as a "PCMCIA bridge device." These PCMCIA-on-a-stick solutions work just as well as their PC Card brethren. The vendors making these PCI and ISA solutions are trading off design time for cost of deliverables. That is, does the vendor sell enough PCI and ISA cards to justify creating a lower-cost, integrated design? The answer, it appears, is no. None of the vendors participating provided an ISA or PCI adapter that didn't eventually present a PCMCIA bus to the host-proof that wireless LAN is still aimed primarily at mobile applications.

The 340 Series Access Point is a breeze to use. In terms of management features, this little package has it all, offering options for telnet, Web-based management and serial-based configuration. The hardware is easily mountable. Cisco supplies all the hardware for a professional installation at your business. We had no problems getting this unit up and running. Unfortunately, the hardware affords no place on which to attach external antennae; its dual diversity antennae are permanently affixed to the access point. Cisco didn't provide us with its detachable-antenna model. We had no problems roaming our call center using a single **wireless access point**.

The access point and PC Cards support 40- or 128-bit encryption. These features are configurable by a license key, which must be bought with the features in mind—that is, you pay only for what you need but don't get the flexibility of everything at a single price.

Cisco Aironet 340 Series Access Point (AIR-AP342E2C), \$1,299; Cisco Aironet 340 Series PCI Adapter (AIR-PCI342), \$349; Cisco Aironet 340 Series PC Card (AIR-PCM342), \$249, Cisco Systems, (800) 326-1941, (408) 526-4000; fax (408) 526-4100. www.cisco.com

Enterasys Networks RoamAbout Solution

Grade: A-

Tied for second place with Lucent's Orinoco, Enterasys Networks' RoamAbout 6.0 Access Point is a powerful wireless solution. Like Cisco's solution, the RoamAbout access point is built with the enterprise user in mind. A serial port can be used to configure the access point initially. Once the unit has been configured, remote configuration is supported via telnet or the provided SNMP utility.

The RoamAbout is one of the most feature-rich access points we tested. The hardware has support for power over Ethernet, which is accomplished by using spare pairs in the Category 5 cable. This greatly simplifies installation in locations where power is not readily available. But you need to be careful with this technology, too: It isn't particularly intelligent, and it most certainly cannot be run through a repeater or a switch. Power over Ethernet is a sort of last-mile power and wire solution designed to simplify wireless installations.

Furthermore, the RoamAbout is the only product we tested that lets you use the remote-power feature as a redundant power source, enabling truly mission-critical wireless networks.

The Enterasys access point uses a PC Card adapter to provide wireless-radio functionality. Thus, as the industry progresses, you can upgrade the wireless radio to the latest technology—a feature shared with products from Lucent and Intermec Technologies. The access point allows a high degree of wireless LAN configurability.

Unlike the PC Cards, the Enterasys access point is not an OEM product. The access point is robust and includes serial and host-based management features, as well as telnet access. Still, like most of the solutions we tested, Enterasys' RoamAbout lacks a complete management package tailored to dozens or hundreds of access points and users.

Enterasys resells the wireless Orinoco PC Card to deliver wireless connectivity both to the access point and to the PC. Like the Lucent card, Enterasys' product delivers performance well above average, and its power consumption and range were among the best we tested.

RoamAbout 6.0 Access Point, \$999; 40-bit Encrypt card, \$199; 128-bit Encrypt card, \$249, Enterasys Networks, (603) 332-9400; fax (603) 337-2211. www.enterasys.com/wireless or sales@enterasys.com

Lucent Technologies Orinoco Wireless Networking System for Enterprise Network Computing Best Value

Grade: A-

Lucent's Orinoco Wireless Networking System for Enterprise earns Network Computing's Best Value award by lowering the bar on wireless pricing. At \$179 for Orinoco PC Cards, Lucent's solution costs \$20 per card less than its closest competitor and represents a phenomenal improvement over the \$500 to \$800 per-unit pricing of just a year ago. Lucent's Orinoco PC Card has an integrated antenna; however, it also sports a small accessory connector that can accept an external wireless antenna. Lucent's and Enterasys' solutions were second to Cisco's by a very thin margin. The ease of management and raw performance provided by the Aironet 340 Series gave it a slight edge over Lucent's Orinoco.

Orinoco is a 5-volt PC Card. Lucent provides drivers for almost every operating system, including all flavors of Microsoft Windows, Windows CE, DOS, Linux and Apple MacOS. The Lucent solution is the most widely supported adapter of all the units we tested, a boon for sites with multiple operating systems to support. Lucent's Orinoco took second place in our performance tests, with an average of 4.5 Mbps of throughput and a top throughput of 4.9 Mbps. Orinoco's power utilization under standard operating conditions was the lowest of all the 5-volt cards we tested; when

we enabled power-saving mode, it performed extremely well, using only 75 milliwatts of power in quiescent mode, the second lowest of all the products we tested.

The Lucent Orinoco access point features a dual-slot PCMCIA design. This design, Lucent claims, gives you a number of options, including migration from previous wireless technology/standards or, alternatively, a way to improve performance or fault tolerance within a single cell. The access point takes the same Orinoco cards that are installed in notebook computers. It can also be a wireless bridge (building to building) with the extra slot.

The Orinoco access-point management software is functional, but not fantastic. Lucent has been using the same wireless-access configuration software for years; it **discovers access points** on the network and then lets you configure most of the operational parameters on a per-access-point basis.

Basic access-point features as well as specific wireless parameters are configurable from a single interface. However, only one access point can be managed at a time.

The Orinoco access point checks in at under \$1,000. However, Lucent hides some of the cost of its solution in packaging. The Orinoco access point does not come with a wireless PC Card. You must purchase the PC Card separately, putting the cost near \$1,200.

Orinoco Wireless Networking System for Enterprise, \$995 for WavePoint II access points, \$179 for Orinoco PCMCIA cards, Lucent Technologies, (800) WAVELAN, (973) 581-4297; fax (973) 581-3223. www.wavelan.com or vonschaumbur@lucent.com

3Com Corp. 3Com AirConnect 11 Mbps Wireless LAN

Grade: B+

3Com's AirConnect 11 Mbps Wireless LAN product is a pleasure to use. The AirConnect PC Card we received came in a starter pack, which includes three of the wireless PC Cards and a **wireless access point** for just under \$1,800. The AirConnect PC Card is actually an OEM unit from Symbol Technologies. The card features a modular detachable-antenna design. We speculate that excessive wear on the antenna/main body could damage the delicate hinge between the wireless PC Card and the antenna. If you're looking for extra range, you can remove the modular antenna and instead attach an external special-purpose antenna.

In our tests, the 3Com wireless PC Card performed admirably, coming in just behind Lucent's and Cisco's products, with a peak throughput of 4.6 Mbps and an average of about 4 Mbps.

The 3Com client is one of the best we tested; it includes support for Mobile IP, which lets you roam among multiple subnets, a handy feature in a typical, routed enterprise infrastructure. 3Com is also the only vendor that let us specifically choose an access point, rather than having the software just pick the strongest access point. This flexibility is a valuable feature if you are trying to manually segregate your traffic to balance network load. Although it's tedious to configure mobile users, once configured, they can roam just as other users can. You can also automate the process by forcing the user to join a particular network area using the 802.11b ESSID (Extended Service Set ID) field. We still wish there were a better way of associating users to access points.

The 3Com access point boasts a large fixed-configuration antenna. Upon closer inspection, we found the access point actually contains a PC Card radio with a special antenna fixed to the PC Card. That card does not appear to be removable.

Configuration and monitoring tools on the 3Com access point are extremely flexible and a snap to use. Like Enterasys' RoamAbout, AirConnect also supports a power-over-Ethernet technology, which lets you place the access point anywhere you can place an Ethernet port. You can manage the 3Com access point from a serial connection, telnet or Web interface. The management interface also lets you manage multiple access-point configurations from a single access point. You can save a configuration or update firmware from one access point to all access points on your network (Cisco's Aironet also supports this feature). We found this feature to be potentially useful but a bit buggy when it came to firmware upgrades. We

hope 3Com will work these bugs out in a future code release. Unreliable code is worse than not having the feature at all.

3Com AirConnect 11 Mbps Wireless LAN, starts at \$1,795 for the starter pack of one access point and three PC Cards, 3Com Corp., (800) NET-3COM, (408) 326-5000; fax (408) 326-5001. www.3com.com

Intermec Technologies Intermec 2101 Universal Office Access Point Solution

Grade: B

Intermec provided us with a unique wireless solution that includes its Intermec 2101 Universal Office Access Point and a 3.3-volt Orinoco PC Card. Intermec's hardware relies on external antennae, which have advantages and disadvantages. Having an external antenna on a wireless PC Card offers the opportunity for extended range and performance, but it also requires a small wire to run from the PC Card to the external antenna. In a typical environment, the external wire is both cumbersome and prone to damage. We see the Intermec solution being used primarily in applications in which users are not mobile but require wireless technology to provide connectivity.

The Intermec **wireless access point** is a two-port PCMCIA-based wireless solution, in some ways similar to Lucent's Orinoco **wireless access point**. Like the wireless PC Cards in the workstations, however, Intermec uses external antennae for its access-point product. The Intermec **wireless access - point** product is easier to configure than the Lucent product; the 2101 features a serial port and telnet and Web-based interfaces to configure and manage the device. However, Intermec's access point is almost twice as expensive as the other products in this review. Historically, Intermec has delivered rugged products designed for outdoor use. However, this access point has a simple plastic design, certainly not suited for the industrial applications at which it seems to be aimed.

Intermec's performance was very middle of the road, with average throughput of around 4 Mbps. On the positive side, the wireless client had the lowest quiescent power utilization-only 53 milliwatts.

Intermec 2101 Universal Office Access Point, \$2,090; Intermec 2102 Access Point, \$950; Intermec 2126 PC Card, \$229, Intermec Technologies, (800) 347-2636, (425) 348-2600; fax (425) 355-955. www.intermec.com or info@intermec.com

Compaq Computer Corp. WL100, WL200, WL300, WL400 Wireless LAN Solution

Grade: B

Compaq presented us with a complete wireless networking solution that included access points, PC Cards, PCI cards for desktop systems and a unique software **wireless access point**. Compaq's package appeared to have all the right pieces, but the performance and range just weren't there.

Compaq's wireless PC Card is 3.3 volts and is manufactured by Intersil Corp. In our tests, the Compaq card had the lowest overall performance. In our call-center range tests, the wireless signal dropped off almost completely at the center of our coverage area. Whether this is the fault of drivers, antennae, access points or the PC Card itself, we were unsure. Compaq lauded the card as having superior 3.3-volt technology, citing the way it integrates with the end-to-end solution, including Compaq's handheld personal organizer. In our tests, the 3.3-volt card did use far less power than some devices, but its power utilization was mediocre-759 milliwatts during quiescent operation with power saving enabled.

Compaq's access point is a NoWires Needed OEM product. The access point is manageable only via the NoWires Needed management software, which-as we mention below-isn't particularly user friendly. The access point is a fixed-configuration device, with no removable (PCMCIA) radios.

One impressive product in the Compaq solution is the software access point. Rather than spending upward of \$1,000 per access point, you can turn any spare PC into a fully functional access point with this software. Using Compaq's WL200 11 Mbps Wireless LAN PCI Card, you can build a **wireless access point** for less than \$325 (compared with \$899 for the hardware access point). The **wireless access - point** software can significantly

lower the total cost of ownership of a wireless solution and can be an ideal SOHO solution, given that every PCI NIC is bundled with a standard-license edition of Deerfield.com's WinGate, which is a popular NAT (Network Address Translation) and proxy software package. Our tests showed the software access point is just as functional as a hardware-based access point in terms of performance and interoperability.

WL400 11 Mbps Wireless LAN Hardware Access Point, \$899; WL100 11 Mbps Wireless LAN PC Card, \$199; WL200 11 Mbps Wireless LAN PCI Card, \$199; WL300 11 Mbps Wireless LAN Software Access Point, \$125, Compaq Computer Corp., (800) 345-1518; fax (281) 518-1442. www.compaq.com

The NoWires Needed 11 Mbps Wireless LAN
Grade: B

The NoWires Needed 11 Mbps Wireless LAN solution we tested was an early beta. During the course of our tests, the company was purchased by Intersil (the company that makes the Prism chipset). NoWires Needed is an OEM provider of wireless equipment for several of the LAN wireless vendors, including BreezeCom and Compaq. However, the equipment we tested was a different generation and model than the OEM equipment the company provides to other vendors.

The 5-volt wireless PC Card provided by NoWires Needed has a fixed-antenna construction. In our lab tests, the NoWires Needed card turned in the best encrypted performance-it was the only card to come in above 5 Mbps with encryption enabled. Furthermore, this card has great power-utilization statistics. The NoWires Needed product doesn't have a power-saving "mode"-it always operates in power saving. Power consumption in quiescent mode was about 150 milliwatts-lower than many of the competitors' results in power-saving mode.

The NoWires Needed driver suite is a bit sparse in terms of diagnostic tools. However, NoWires Needed took the extra effort to provide highly visible encryption warnings and information, a detail the other vendors overlooked.

The NoWires Needed access point is small but effective. Integral to the NoWires Needed solution are the options for 40-bit or 128-bit encryption, or NoWires Needed's own 128-bit AirLock security. A public/private key exchange system that eliminates the need for distributing shared keys in an encrypted environment, AirLock is an unusual and innovative feature that takes wireless security to a new level. Of course, AirLock is proprietary, and it prevents people only from "sniffing" your wireless data from the air. AirLock's key negotiation eliminates one aspect of security by not requiring the user to enter a public key. We think the trade-off of keyless security is well worth the lack of public keys. Fortunately, NoWires Needed hasn't ignored the need for standards-based encryption. If AirLock isn't available, the client will drop back to standard 40-bit or 128-bit encryption as the environment provides.

NoWires Needed provides management software to configure and monitor access points. However, we weren't impressed by the NoWires Needed management tool, which is also used by several NoWires Needed OEMs. The management software keeps its own state, which didn't always match the state of the access point, making management cumbersome. The software often didn't reflect the state of the remote access point, and sometimes changes we made weren't represented on the remote device.

Priced at \$219 for a client PC Card and \$999 for the Enterprise Access Point, the NoWires Needed solution is a solid performer and a good bargain.

NoWires Needed 11 Mbps Wireless LAN, \$219 for PC Card, \$999 for Enterprise Access Point, \$499 for Small Business Access Point, NoWires Needed BV, +31-30-229-60-60, (650) 330-1466. www.nowiresneeded.com or info@nwn.com

Farallon Communications SkyLine 11 Mb Wireless PC Card
Grade: B-

Farallon Communications is yet another vendor offering a wireless 802.11b high-rate PC Card, but the company does not make an access-point product. We recently tested Farallon's 802.11b wireless product on the Macintosh in our Real-World Labs(r) at the University of Wisconsin-Madison

(see "Farallon's Faster SkyLine Does Mac and Windows, Too," at www.networkcomputing.com/1112/1112sp4.html). Here we find it again; however, this time the tests focus on the Wintel platform. The Farallon SkyLine 11 Mb Wireless PC Card is an Intersil OEM product, but Farallon has done additional development to provide support for the Mac. Note that this is not the recently acquired NoWires Needed product we cover above, but another (older) Intersil reference design.

In the lab, the Farallon card performed around the top end of average, with a maximum throughput of 4.5 Mbps and an average of around 4.2 Mbps. WEP-encrypted performance was respectable, too, with top throughput exceeding 4 Mbps and average throughput of around 3.8 Mbps.

The Farallon card has an integrated antenna and driver support for MacOS and Windows 95/98 and NT 4. At \$199, Farallon's SkyLine is competitively priced.

SkyLine 11 Mb Wireless PC Card, \$199, Farallon Communications, (800) 613-4954, (510) 346-8000; fax (510) 346-8119. www.farallon.com or info@farallon.com

Zoom Telephonics ZoomAir Wireless Networking

Grade: C+

Zoom Telephonics also provided us with a wireless PC Card. The ZoomAir Wireless Networking card is actually an Intersil OEM product. Zoom's product matches Lucent's in price, coming in at a low \$179 per card. The ZoomAir is a 5-volt card with a permanently attached antenna. As we mention in "Top 10 Things To Know About Wireless" (see www.networkcomputing.com/1113/1113f2side2.html), the wireless industry is dominated by a small number of hardware manufacturers. The difference in OEM products comes in antenna design as well as driver implementation.

In the lab, ZoomAir's unencrypted performance was on the low end, averaging about 3 Mbps. With encryption enabled, however, the Zoom card zoomed right along, delivering the fourth-best performance of all the products we tested—a solid 4 Mbps.

ZoomAir's installation procedure is meant to be idiot-proof, but it was designed poorly. To install ZoomAir's drivers, you must use the company's setup utility, which installs IP, IPX and NetBEUI protocol support on your operating system whether you want it or not. Of course, you can remove these protocols, but there is no reason the install should unnecessarily add them to your operating system.

Zoom also offers a software access point, but because the company didn't have a PCI card ready in time for our review and provided only two PC Cards, we were unable to test that product in our lab.

ZoomAir Wireless Networking, \$179, Zoom Telephonics, (800) 631-3116, (617) 423-1072; fax (617) 423-3923. www.Zoom.com or sales@zoom.com

BreezeCom DS.11 Wireless Solution

Grade: C+

BreezeCom provided us with its AP-DS.11 Access Point 2.4.0 and SA-DS.11 Station Adapter 2.4.0 solution. Unlike the other vendors, BreezeCom did not provide us with any PC Card adapters. Instead, its station adapter looks like a standard access point but provides Ethernet-to-wireless connectivity to a wireless network, which is just the opposite role that an access point plays.

And unlike some of the other products we tested, BreezeCom's DS.11 solution offered no encryption and no power-saving mode. Then again, because the units must be plugged into the wall, power saving really isn't an issue.

Managing the DS.11 hardware is done from BreezeCom's GUI-driven SNMP manager. Like most of the configuration and monitoring tools we tested, this one was a little clunky. We had a hard time getting it going, but once we figured out the nuances, we were able to configure the hardware appropriately. The performance of the DS.11 was average at around 4 Mbps.

AP-DS.11 Access Point 2.4.0, \$1,195; SA-DS.11 Station Adapter 2.4.0, \$795, BreezeCom, (760) 517-3100; fax (760) 517-3200. www.breezecom.com or sales@breezecom.com

Zcomax Technologies XI-300 11 Mbps Wireless PC Card

Grade: C+

Zcomax Technologies provided us with its XI-300 11 Mbps Wireless PC

Card. The Zcomax hardware features a detachable antenna, with a construction similar to that of the 3Com card. Zcomax informed us, however, that it is a top-level hardware provider; that is, it makes its own PC Cards and is an OEM provider to other manufacturers. Power consumption for the XI-300 was much higher than the competition's-1,225 milliwatts in quiescent mode. Performance was average, around 4 Mbps in our client-server tests.

The Zcomax card does not support encryption, so we were unable to test that feature. We spoke with Zcomax about XI-300's power utilization and performance and found out the company is releasing a new driver, but that driver was not available for our tests. The old driver did not have power-saving mode implemented, even though it was an option in the controls; that explains the poor power utilization.

XI-300 11 Mbps Wireless PC Card, \$199, Zcomax Technologies, (562) 926-4588; fax (562) 926-7885. www.zcomax.com or sales@zcomax.com
<http://www.nwc.com/>

Copyright (copyright) 2000 CMP Media Inc.
COPYRIGHT 2000 CMP Media, Inc.

COMPANY NAMES: Cisco Systems Inc.--Products; Lucent Technologies Inc.--Products; Enterasys Networks--Products; 3Com Corp.--Products; Intermec Technologies Corp.--Products; Compaq Computer Corp.--Products; NoWires Needed--Products; Farallon Communications Inc.--Products; Zoom Telephonics Inc.--Products; BreezeCOM Inc.--Products; ZCOM Inc.--Products
GEOGRAPHIC CODES/NAMES: 1USA United States
DESCRIPTORS: Hardware multiproduct review; Wireless LAN/WAN system
EVENT CODES/NAMES: 350 Product standards, safety, & recalls
PRODUCT/INDUSTRY NAMES: 3662116 (Wireless Local Area Networks)
SIC CODES: 3663 Radio & TV communications equipment
NAICS CODES: 33422 Radio and Television Broadcasting and Wireless Communications Equipment Manufacturing
TICKER SYMBOLS: CSCO; LU; COMS; CPQ; ZOOM
TRADE NAMES: Cisco Systems Aironet 340 (Wireless LAN/WAN system)--Evaluation; Enterasys RoamAbout (Wireless LAN/WAN system)--Evaluation; Lucent Technologies Orinoco (Wireless LAN/WAN system)--Evaluation; 3Com AirConnect (Wireless LAN/WAN system)--Evaluation; Intermec Technologies 2101 Universal Office Access Point (Wireless LAN/WAN bridge/router)--Evaluation; Compaq WL (Wireless LAN/WAN system)--Evaluation; NoWires Needed 11 Mbps Wireless LAN (Wireless LAN/WAN system)--Evaluation; Farallon Communications Skyline (Wireless LAN/WAN adapter)--Evaluation; Zoom Telephonics ZoomAire Wireless (LAN/WAN adapter)--Evaluation; BreezeCOM BreezeNET AP-10 (Wireless LAN/WAN bridge/router)--Evaluation; Zcomax Technologies XI-300 (Wireless LAN/WAN system)--Evaluation
FILE SEGMENT: CD File 275

13/9/6 (Item 6 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2005 The Gale Group. All rts. reserv.

02384654 SUPPLIER NUMBER: 60372332 (THIS IS THE FULL TEXT)
WIRELESS LANS -- LOOK, MA... NO WIRES -- Wireless networking products prove they are finally ready for prime time.(Hardware Review)(Evaluation)
Rist, Oliver; Chee, Brian
InternetWeek, 41
March 20, 2000
DOCUMENT TYPE: Evaluation ISSN: 1096-9969 LANGUAGE: English
RECORD TYPE: Fulltext
WORD COUNT: 5927 LINE COUNT: 00466

TEXT:

Until recently, wireless LAN devices have been regarded as niche-class products, or even just frivolous executive toys. But after the 802.11 High Rate specification (known colloquially as 802.11b) was finalized, vendors finally had a real selling point, namely 11 Mbps' worth

of viable throughput. Hang onto your hats; wireless just got useful.

To get the skinny on the new wireless LAN (WLAN) segment, we issued our typical product-test call and got responses from five brave vendors. Most of these are pioneers in wireless LAN technology, because even though the 802.11b specification has been around for a year and is generating lots of industry buzz, you'll still see a number of product ship dates occurring in the second quarter of this year.

3Com sent a final preproduction edition of its AirConnect series. Aironet sent its mature and shipping 4800 series, followed by Cabletron's almost-as-mature RoamAbout line with the 11-Mbps upgrade. Lucent also sent its shipping 11-Mbps WaveLAN products. The last vendor included in this comparative review, Compaq, needs to be considered separately because they shipped an earlier level of the beta product than anyone else.

Nokia and Zoom were invited to participate, but neither responded in time for testing.

While functional, Compaq's WL series shouldn't be evaluated for purchasing based on this review-at least not until you've had a chance to experience the final shipping version. Judging from the direction Compaq has taken with the WL, these devices should be impressive and available by the time you read this, although we were unable to acquire such units in time for testing.

The State Of Wireless

As far as the state of the WLAN market is concerned, our advice is to tread carefully. For the most part, these products worked-and worked well. But they did so only within their own product families, meaning you're much better off purchasing PC Cards, hardware access points and management software from the same vendor-at least for now.

In fact, some rumormongers are saying that you're safest running these products not only within the same WLAN vendor family, but also with hardware from the same wired-network manufacturer (3Com's AirConnect with 3Com's OfficeConnect hubs and switches). But we're here to tell you that this just isn't the case. All these products were plugged into Intel or Cisco hubs and switches during testing and never encountered a problem. We found excellent results with backward compatibility, too. Using older, 2-Mbps 802.11 equipment from Bay Networks proved easy and reliable. But if wireless is so sunny, why the warning to tread carefully? The same old saw: competing standards.

While 802.11b is the corporate networking wireless medium of choice, it is facing competition and legislative battles from other standards, namely HomeRF and Bluetooth. Basically, high-speed wireless networking plays only in the 2.4-GHz frequency band. That's a problem because this band is limited to only 60 to 80 discrete channels at 1 Mbps, dropping savagely to only 3 channels at 11 Mbps. Stick three competing standards in there, as well as a slew of 2.4-GHz cordless telephone products, and you have trouble.

To summarize, 802.11b devices use Direct Sequence Spread Spectrum (DSSS) transmission, while HomeRF uses Frequency Hopping Spread Spectrum (FHSS). The major difference is that FHSS sends data over a 1-MHz carrier that "hops" from frequency to frequency within the 2.4-GHz band about 50 times a second. DSSS, on the other hand, stays fixed within a 17-MHz carrier channel, but sends out a lot of noise to cover that range, with its devices able to pick relevant data out from among this cyber fog. Finally, Bluetooth also uses FHSS transmission, but at a much more accelerated hopping rate than HomeRF.

Even though each standards body is using a different transmission methodology, they're still forced to compete for space and regulatory advantage with the FCC in order to provide longevity to their product lines.

At the moment, 802.11b is in the lead for corporate WLANs, but Bluetooth will be a big player in the personal area network market-meaning wireless connections between PDAs and desktops, laptops or printers. This may sound like home networking, but the PDA angle implies that users will want to run Bluetooth networking while in the office, making the resolution of Bluetooth and 802.11b a serious matter for network managers intent on deploying this technology right now. A similar quandary exists for

telecommuters who standardize on HomeRF in their den, then want to take their notebooks on visits to the corporate headquarters.

Security And Room To Roam

Another sticking point in the WLAN specification is security. With hackers making the national headlines weekly, protecting wireless data streams is of the utmost importance. Vendors have answered this call with the Wireless Equivalent Privacy (WEP) encryption standard. They've even bolstered WEP's initial 40-bit encryption key to a meatier 128-bit key in recent product releases after a relaxation in encryption legislation. This looks great on paper, but we found other security problems that vendors haven't yet answered.

For one, with only three channels operating in an 802.11b scenario, building a device to jam all of them wouldn't be all that difficult. Indeed, the same denial-of-service attacks that have been busily frying Web servers the last few months could also be used to drain battery life from WLAN-dependent devices.

Some security experts will quickly point out that devising such an attack on the products tested here (the 802.11b camp) would be more difficult than we make it sound. First, hackers would have to find the appropriate radio frequency signal, which would typically be below ambient noise level in a DSSS transmission scheme. Then that signal would have to be rebuilt, which means breaking the 40-bit (or now 128-bit) encryption process. And then a hacker would still need an appropriate ESSID and IP address.

Again, that sounds difficult, but we encountered situations in testing that reveal it may be easier than you'd think. While testing Lucent's cards, we found that the PC Card WLAN Network Interface Cards (NICs) could use an ESSID browser, which basically polls the local area for any access-point device, then attempts to sync up. Left in default mode, some access points will automatically accept these newcomers. Considering that Lucent is the basis for Apple's AirPort WLAN series and is also very similar to Cabletron's RoamAbout series, this security hole covers a wide range of product types.

Then there is the question of roaming. When a wireless NIC accesses the network, it typically registers with a single **wireless access point**. But since wireless equals mobility, network managers must expect users to move around. Indeed, since most access points are rated for only 60 or 70 simultaneous users, network managers will want them to move around to save their access points from overload.

But what happens to users' connections when they move from one access point to another? In the cellular telephone world, this has often meant becoming disconnected if access points aren't spaced properly. And the data world adds additional complexity, namely that each access point must be wired into local networking hardware. This means that access points in different departments, different floors or even different buildings will most likely be on different subnets.

That represents a singular challenge to wireless LAN manufacturers in that the users' networking experience can't be interrupted with a new login screen every time they stray across subnets. Shockingly, no wireless vendor is presently capable of addressing this problem. Our testing showed that for roaming within the same subnet, these devices worked great. Handoff was seamless as long as proper overlap was maintained between access points.

But roaming across subnets is still an unanswered issue, and that's a critical weakness for enterprise deployment and one you should check out carefully before making any purchasing decisions. At the moment, there are only two ways around this problem. First, users will need to reconfigure their IP settings whenever they walk across subnet boundaries-not very attractive in most situations.

The second has a much better result, but requires the proper equipment in your data center. We're talking about placing all the access points on their own subnet, in effect creating a VLAN for only wireless users. But to do this, you'll need Layer 3 switches in your network capable of 802.1p tagging.

We tried this scheme ourselves at a recent Network+Interop trade show, where access points were scattered all over the trade show floor and

even some of the hotels, and had no trouble with roaming. But it sure was a far cry from plug and play. The bottom line: Be sure to plan carefully before attempting to integrate these devices into an existing enterprise campus.

Are They Ready?

So, with all these issues, are WLANs really ready for prime time? After testing these products for the last few months, we'd have to say yes, regardless of standards wars or security problems.

For one thing, the upgrade to 128-bit WEP encryption should severely slow down most cracking attacks, and vendors are continuously working to improve security in other ways. The same goes for standards implementation. Vendors like 3Com, Cabletron and Lucent all confirm their ability to keep pace with the standards war using only software or firmware upgrades, while keeping hardware-purchasing dollars safe. And while roaming issues pose a problem now, vendors are working on easier solutions even as we speak. In the meantime, you can work around it as long as you have the proper back-end equipment.

With throughput speeds competitive with 10Base-T and prices coming down from the stratosphere, we feel that these new wireless networking products can save you real money in many situations by avoiding wiring costs, as well as man-hour dollars for complex installations.

Using WLAN technology, IT departments can literally configure an entire remote office network at the central data center. Then they can send via overnight delivery notebooks, desktops, printers and access points to remote locations and simply have users turn on their devices. Presto! Instant network. Extend that scenario out to temporary offices, trade show and convention floors, and even executives who can't stay planted behind a desk, and you get the full picture. Sound the call; wireless LANs have grown up.

3Com AirConnect

In typical 3Com fashion, its AirConnect products are not only well made, but ambitious in scope. These devices have a competitive price and solid base performance. And 3Com has gone the extra mile in several areas pertaining to management and standards compliance. Unfortunately, the products we reviewed were late beta versions, although 3Com assured us that the hardware was production level. Even so, we encountered some difficulties with the installation software. Also, we were unable to test roaming because one of the access points died midway through testing.

When everything was functioning, however, you wouldn't have known these were beta-level products. 3Com begins its installation procedure with the advice to run a utility called Site Survey, which records the wireless connection quality at the installation site and uses this information to recommend an optimal number of access points for complete site coverage. Within our test space, this utility was superfluous, but it did give us good advice as to access-point placement-certainly useful in large office environments.

Installing 3Com's AirConnect access point was definitely the most difficult part of the installation process. 3Com has gone to great lengths to make these devices highly manageable and secure in a corporate environment, but the flip side of that coin is that you'll need to be familiar with these devices to configure them. That is made more difficult by 3Com's online-only documentation, which was quite terse and omitted random sections of instruction. Yes, it's terribly analog of us to yearn for paper documentation in this day and age, but online documents have never lived up to print quality in our experience, and 3Com's was no exception.

Initially, you'll need to connect via a serial cable and a terminal interface running at 19.2 Kbps. Unlike products that were easier to set up, such as the Aironet, this step involves setting up not only the access point's IP information, but security IDs and acceptable client configurations based on the Message Authentication Code (MAC) address. Frankly, 3Com isn't the only vendor in this roundup to fall back onto MAC addresses as a configuration step, but even so, we were disappointed. While there are certainly technical reasons for defaulting to MACs, we felt this was unnecessarily granular and unpolished for today's corporate

environments.

Additionally, the only way we were able to get this device to work in a network running DHCP was to provide it with a static IP address, then disable this address in the DHCP server. 3Com's documentation indicated that the device supported DHCP, but like the Compaq WL series, attempting to connect this way crashed our DHCP server every time. Later, it turned out that this was due to our use of Ositis's WinProxy 3.0 as an Internet gateway server-cum-DHCP server and firewall. When we switched to Windows NT Server's native DHCP service, things ran smoothly.

Once the access point was configured, things took a turn for the better. Remote management of the access point offers a plethora of choices. 3Com's product includes a dedicated network-management tool, as well as the ability to integrate the AirConnect devices into its own Transcend network and systems-management framework. Additionally, you can also telnet into the device or use other network-management frameworks, as long as they support SNMP.

PC Cards installed with no problems, and we were up and connected on both test notebooks within 10 minutes of installing the access point. Throughput performance was in line with the rest of the pack, although distance wasn't as great as that of the Aironet. On the other hand, 3Com doesn't claim a 500-foot max distance, just 300 feet in typical office environments. Our connected wanderings bore out this claim and with an additional benefit over the Aironet. Where the latter simply disconnected when taken beyond its range limit, 3Com's AirConnect actually defaulted to its 2-Mbps speed first. This allowed us an extra 100 feet or so of traveling distance before the device disconnected.

Additionally, 3Com claims compliance not only with 802.11b (or 802.11 HR), but also the upcoming Wi-Fi standard. It intends to deliver this compliance to existing AirConnect customers via free software upgrades.

While its price may not be the cheapest in this roundup, it's also not the most expensive. 3Com's extensive management and security capabilities make the extra money more than worthwhile. Once this product passes its beta stage into a more polished final version, it should definitely be considered for any WLAN installation.

Aironet 4800 Series

The Aironet 4800 is actually a pioneer in the 11-Mbps space, having arrived as one of the first 802.11b-compatible products available anywhere. But while its maturity shows both in performance and ease of setup, its documentation and management utilities are a bit on the bare-bones side.

Aironet's kit is much like the Compaq WL series in look and feel. Access points look a lot like the handset for a 2.4 GHz phone, with two antennas mounted on either side and the ability to run as tabletop or wall-mounted units. Aironet thoughtfully included a pillar mounting bracket, designed to easily mount an access point on an office support pillar or cubicle frame.

Again, easy configuration is exactly what Compaq was aiming for and fell short of due to their beta-level products. The access point simply acts as an extension of a hub or switch. Unlike Compaq, initial configuration of the access point is done via an included serial cable and a terminal program on a system manager's notebook.

This may sound like a bit of a problem if you're intent on shipping these out to remote offices with little or no support help, but remember that the access points can be preconfigured before shipping to these locations. And even if they're not, the terminal program is as easy as the rest of Aironet's installation procedures, so it would be easy to walk a user through the process over the phone.

Initial setup consists of assigning the access point an ID name, setting a maximum allowable bit rate and assigning the box an IP address. Once these steps are completed, you can pretty much toss the serial cable out the window, as future configuration chores can be handled via a Web browser.

Interestingly, once we configured the Aironet access point via the serial connection, it was able to plug into our DHCP-served test segment with no hassles-unlike the Compaq device. While we still don't have an official explanation of what happened with the WL series and our WinProxy

DHCP server (see the Compaq review on page 50), this result would seem to indicate that Compaq's access point was in the throes of attempting to identify its configuration host and, in doing so, crashed the DHCP service. Aironet's approach of manual configuration, while not as elegant as the auto-find feature in the WL, seems a bit more reliable.

Installing Aironet's PC4800 wireless NIC in our Compaq Presario 1920 and Micron XKE test notebooks was the same as installing any other NIC. Under both Windows 98 and Windows 95, installation was flawless, as long as we had the appropriate driver diskette.

While you can set the PC Card's bit rate manually at this stage, we found it easier to leave it at its default setting, which synchronizes automatically with the nearest access point.

Performance on our Ganymede Chariot 2.1 throughput tests was in line with the rest of the competition in this roundup. At the Aironet's maximum bit rate of 11 Mbps, actual application traffic averaged between 5 Mbps and 7 Mbps of real throughput. Distance measurements were exceptional, however, as we were able to maintain this level of traffic by as much as 375 feet and through a wall. Moving the access point back behind a second wall, however, caused the PC to lose its connection, forcing us to re-enter the lab before a connection was re-established.

Overall, Aironet gave us easy installation and solidly competitive performance. From an IT manager's perspective, we would have liked it if the package included more in the way of systems-management tools besides its standard support for SNMP, as well as better documentation. This would be especially useful when integrating this product into an existing IT infrastructure. We hope this will change soon now that Aironet has been acquired by Cisco.

Cabletron RoamAbout

Where 3Com, Aironet and Compaq had a similar product feel, the Cabletron RoamAbout was more similar to Lucent's WaveLAN series in terms of product configuration and features-although not so similar in terms of price. Cabletron definitely comes up the winner on the dollar front in this roundup, with a cost of \$799 per access point and only \$199 per PC Card interface (with basic WEP encryption).

You get a lot of functionality for your money with this series, including excellent management support, competitive performance and great security. You even get a nice set of printed manuals, which was hard to come by in this roundup.

As with all of these devices, most of you will sweat while setting up the RoamAbout access point. Like Lucent's access points, these come with a large metal mounting bracket for wall mounts, as well as little rubber feet for desktop mounts. You'll also need to install a remote power link that connects to the access point via a proprietary power cable and a Cat. 3+ networking cable on one side while connecting to your wired network and a power outlet on the other.

This may seem like an added inconvenience-and in some basic situations it is-but in large offices it provides not only more flexibility in terms of distances from power outlets and wiring closets, but it also keeps the giant black power cables from creeping all over your walls. We didn't like the fact that all this bracketing hardware is big. It sticks out about two inches from the wall, which means you'll need to mount it fairly high to keep it out of your way.

Once this wiring step has been arranged, you'll run into the second biggest difference between the Cabletron/Lucent camp and the others in this roundup: Their access points require the use of one of your wireless PC Cards in order to function. This is not a big problem, considering the price tag.

While we're sure that 3Com will give Cabletron a run for its money in the management software department once its products leave beta, during this review, Cabletron was king of the management hill, especially considering the price. Remote management and configuration utilities were polished and deep, and the procedures for use were accurately detailed in the accompanying manuals.

We had a base configuration up in only a few minutes. Again, like the Lucent products, our only gripe here is that we would have preferred to see

a serial interface on the access points. Remote-access configuration is fine, but having to locate the proper access point MAC addresses is a problem-especially in a larger network.

Cabletron has paid special attention to security with this release. One caveat, however, is that we didn't test its ESSID browsing capabilities; buyers should check out this feature before purchasing. Other than that, Cabletron supports everything you'd want from a secure WLAN, including both 40-bit and 128-bit Wireless Equivalent Privacy. It even supports key management so managers can change encryption keys when required. You should be aware, however, that PC Cards are configured for security access in hardware, meaning you'll need to decide whether you want 40-bit encryption or 128-bit encryption before purchasing.

The RoamAbout's throughput performance was excellent as well, with Chariot results running at 5 Mbps or higher and extending the range easily to 400 feet and beyond from the nearest access point. Cabletron rates the RoamAbout out to 550 feet (50 feet longer even than Aironet) and even allows for the addition of high-gain antennas on its access points and cards. This is equivalent to a wireless long-link card, allowing connection at up to 10 miles from the access point in some instances, although typically only at 2 Mbps or slower access speeds.

Cabletron's RoamAbout products provide an excellent and well-polished WLAN solution. And considering the price tag, they're easily the most attractive product family in the roundup.

Compaq WL Series

To be fair, Compaq was caught off guard with this review. It showed up with beta hardware that was not nearly as finished as that submitted by 3Com. The company tried to get us updated hardware, but wasn't able to make it in time for testing. While this certainly caused us some problems, we need to stress at the outset that many of these problems are solely due to the WL's beta nature and won't be there when the product ships. We've noted where we think this won't be the case.

Like Aironet, Compaq is equally targeting both the small office/home office (SOHO) market and the corporate market with the WL series. It's accomplishing this by making its installation process as easy as possible.

Installing an access point should have been as simple as plugging it in and then running the configuration software on a machine wired into the same subnet. The workstation should have found the access point automatically and begun installation.

In our tests, however, this was not the case.

No matter what we tried, Compaq's management software could not locate the WL access point, even when we moved from an Intel Express 550T switched 100Base-T network with four subnets and a couple of VLANs to a single subnet connected via a 10Base-T hub. As there is no serial connector on the WL access point, we couldn't go in and configure it manually.

Additionally-and much like the 3Com device-the Compaq WL immediately crashed the DHCP service running on our smaller test LAN. We never did find out why it crashed, but subsequent testing proved that this shouldn't be a big problem in larger corporate networks. The reason is that our test LAN was running Ositis's WinProxy 3.0 in order to provide a quick sharing gateway to our cable modem-enabled Web access. (WinProxy acts as one-stop DHCP server, proxy server and a firewall, making it a popular choice when configuration time is tight.)

Compaq's WL invariably crashed this service within three or four seconds of being plugged into the switched or hub-connected test LAN. But when we did away with software Web access and ran NT's native DHCP service as well as a Cabletron 245 Smart-Switch router behind the cable modem, the WL ran just fine and managed easy default connections to all its own PC Cards.

Compaq may have some trouble in the SOHO market if it doesn't fix this WinProxy problem in the shipping version of the product, but it won't make much difference in the corporate arena.

Installing Compaq's PC Cards proved to be no problem under Windows 98 or Windows 95. While we were unable to test much of Compaq's security feature set due to our inability to configure the access point beyond its

defaults, we nevertheless managed to achieve connectivity to a range of around 350 feet. But we ran into trouble running Chariot timing records, probably due to our inability to provide a full configuration for the access point router.

On the downside, Compaq's WLAN NIC utilities are overly complex. WEP key generation should be automatic instead of forcing users to press a "Generate" button. Additionally, when the PC Card is scanning for access points, Compaq should have something to indicate activity.

The Compaq WL access point has one thing in its favor, namely that it uses reverse SMA connectors on a pair of external antennas. This allows the radio to better deal with bounced signals by comparing signals and taking the better of the two. It provides a significant advantage in offices with lots of metal in the walls or lined with walls of filing cabinets. Antenna diversity has long been used by ham radio operators to give dramatically better reception. This reverse SMA connector is fairly standard and allows a wide range of external high-gain antennas to be added on in the future.

While Compaq's solution proved problematic for this review, we need to stress again that this basically amounted to an early beta product. Considering its competitive price tag and the elegance that Compaq intends for its eventual release, we'd recommend revisiting Compaq's wireless product line if your WLAN installation plans can wait until their final release.

Lucent WaveLAN

Like Cabletron's RoamAbout series, Lucent's WaveLAN products are also the base OEM platform for Apple's AirPort product line (although rumor has it that this is a slightly dumbed-down version of the original, thus accounting for its low price).

With competitive pricing and solid management, Lucent made an excellent first impression. This was mitigated later, however, when we dug a bit deeper into its security features.

Similar in design to the RoamAbout, the WaveLAN access points have the same heavy, thick wall-mounting brackets and also require you to install a wireless PC Card NIC into each access point. At only \$179 per PC Card, however, this really isn't a big financial burden.

What actually is a bother is how Lucent forces users to configure access points remotely by initially using a supplied MAC address for identification rather than allowing configuration via a serial interface. As the WaveLAN is obviously aimed at larger corporate accounts, this could be a real headache to organize.

Upon installation, the WavePoint access point immediately requests an IP address from a BOOTP server. Unfortunately, it can't get one from a DHCP server-and, yes, this little process caused WinProxy to crash, too. You can work around this by using Windows NT's native DHCP and reserving an IP address for the WavePoint, but this could have been made easier if Lucent had included a serial connection.

Even though we were reviewing shipping products, Lucent neglected to include its WaveManager/AP management software. A little digging, however, quickly led us to the proper URL, where we were able to download it. You should be aware, however, that you must download the remote configuration file menu before you're able to change any access point parameters.

Given that the Lucent platform is also the basis for Apple's AirPort, we decided to check the WaveLAN's Mac compatibility. This was a smooth process since the NICs ran fine in both a Mac PowerPC 1400 running OS 8 as well as a G3 notebook running Mac OS 9. When we installed the same cards in Windows machines, we also experienced absolutely no difficulty.

Things got interesting, however, when we started digging into security, prompted by rumors about wireless security breaches using the AirPort devices at a recent trade show. What we found was that by default, the Lucent WaveLAN cards set their ESSIDs to "Any," and browse the network for any properly configured WavePoints. Upon finding one, they sync their ESSIDs with the closest access point.

It turns out, though, that they'll do this for any wireless access point, including the ones being installed in airports and convention centers around the country.

As long as "any" is specified, both the Apple and Lucent cards will

browse ESSIDs, and that represents a security risk to network managers. Lucent will need to address this problem if it's going to win points with network managers who've sought to protect their networks simply by keeping their ESSID names secret.

Within a single subnet, we found Lucent's roaming abilities worked very well. We especially liked that its "Advanced Configuration" tab in the network control panel contained a setting for low, medium or high user loads for access-point density. This controls how long users can "linger" on an access point before switching, and it's a nice way to keep from overloading a single access point.

Performance was typical for this sector. Throughput generally ran between 5 Mbps and 7 Mbps, although Lucent does rate the WaveLAN out to a 525-foot radius around the nearest access point. Our wandering Web surfer bore this out in testing and even found a seamless drop to 2 Mbps when we moved beyond optimal distance from the access point. This is a nice touch and far preferable to simply disconnecting a hapless user. To increase distance, Lucent supplied each PC Card and access point with the ability to attach an external high-gain antenna, though none were supplied for review.

While its management software is slightly less polished than that of 3Com and Cabletron, Lucent's WaveLAN series is nevertheless a solid choice in terms of performance, security and especially price.

Oliver Rist is contributing technical editor at InternetWeek and technical director at Grand Central Networks Labs. He can be reached at orist@cmp.com. Additional reporting was done by Brian Chee, associate director of the University of Hawaii's Advanced Network Computing Lab. He can be reached at chee@hawaii.edu.

The Rub about Roaming

Because access points have a finite range and WLAN users are generally mobile, users must be able to cross from one access point's area of effect into another's. As long as these access points are on the same subnet, we found this to be no problem. But the industry is still working on a solution for crossing access point territories on different subnets or segments.

Source: The Wireless LAN Association

HITS AND MISSES

AirConnect Series

Hits:

-Polished for late beta products; great pricing; ability to keep pace with upcoming standards and excellent management integration

Misses:

-Hardware problem with one access point; slightly lower distance rating than competition; granular MAC-based initial configuration utility

Aironet 4800 DS Series

Hits:

-Great setup with no hassles; mature product line; standards compliance

Misses:

-Mediocre documentation and no-frills management software

Cabletron RoamAbout

Hits:

-Mature product; no-hassle operation; excellent management integration; good WEP encryption; future standards support and great pricing

Misses:

-Could have benefitted from having a serial connection and a command-line interface for initial configuration; bulky hardware; possible security problem with ESSID browsing

Compaq WL Series

Hits

-Aims for total ease of use with automatic default configuration;

good pricing

Misses:

-Beta-level hardware had configuration and throughput problems;
advanced settings regarding security overly complex

Lucent WaveLAN

Hits

-Very mature product line with good support for future standards;
good pricing; great support for roaming

Misses

-No-frills installation could be easier; management package, while
solid, could be improved; bulky access point hardware; possible security
hole with ESSID browsing

Cabletron RoamAbout

Enterasys Networks/Cabletron

Rochester, N.H.

603-332-9400

www.cabletron.com

PRICING: \$799 access point; \$199 PC Card; \$249

PC Card with 128-bit WEP

AirConnect Series

3Com

Santa Clara, Calif.

800-638-3266

www.3com.com

PRICING: \$1,195 access point; \$219 PC Cards; \$1,795 starter pack
bundle (one access point and three PC Cards)

Aironet 4800 DS Series

Aironet Wireless Communications

Akron, Ohio

800-247-6638

www.aironet.com

PRICING: \$1,995 access point; \$795 PC Card adapter

Compaq WL Series

Compaq Computer

Houston

800-892-6608

www.compaq.com

PRICING: \$199 network adapter (PCI or PC Card); \$899 hardware access
point; \$125 software access point (upcoming software will come with
separately purchased network adapter)

Lucent WaveLAN

Lucent Technologies

Parsippany, N.J.

800-WAV-ELAN

www.wavelan.com

PRICING: \$999 hardware access point; \$179 for base PC Card NIC; \$199
for PC Card that supports 128-bit WEP encryption

<http://www.internetwk.com/>

Copyright (copyright) 2000 CMP Media Inc.

COPYRIGHT 2000 CMP Publications, Inc.

COMPANY NAMES: Cabletron Systems Inc.--Products; Compaq Computer Corp.--

Products; 3Com Corp.--Products; Lucent Technologies Inc.--Products

GEOGRAPHIC CODES/NAMES: 1USA United States

DESCRIPTORS: Hardware multiproduct review; Wireless LAN/WAN bridge/router
; Wireless LAN/WAN adapter; Wireless LAN/WAN system

EVENT CODES/NAMES: 350 Product standards, safety, & recalls

PRODUCT/INDUSTRY NAMES: 3662116 (Wireless Local Area Networks); 3661257
(LAN/WAN Adapters)

SIC CODES: 3663 Radio & TV communications equipment; 3661 Telephone and

telegraph apparatus
NAICS CODES: 33422 Radio and Television Broadcasting and Wireless
Communications Equipment Manufacturing; 33421 Telephone Apparatus
Manufacturing
TICKER SYMBOLS: CS; CPQ; COMS; LU
TRADE NAMES: 3Com AirConnect (Wireless LAN/WAN system)--Evaluation;
Cabletron Systems RoamAbout (Wireless LAN/WAN bridge/router)--Evaluation;
Lucent Technologies WaveLAN (Wireless LAN/WAN adapter)--Evaluation;
Compaq WL Series (Wireless LAN/WAN system)--Evaluation
FILE SEGMENT: CD File 275

13/9/9 (Item 2 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)
(c) 2005 The Gale Group. All rts. reserv.

06393398 Supplier Number: 54813104 (THIS IS THE FULLTEXT)
Wireless Networking -- New standards are making wireless networks much
easier to set up and use-and they cost less, too.(Aironet Wireless
Communications, Bay Networks, Lucent Technologies, RadioLAN wireless
networking products) (Technology Information)

Harbaugh, Logan
InformationWeek, p71
June 7, 1999
ISSN: 8750-6874
Language: English Record Type: Fulltext Abstract
Document Type: Magazine/Journal; Tabloid; General Trade
Word Count: 3110

ABSTRACT:

Aironet Wireless Communications' \$495 PC4500 wireless LAN/WAN adapter and
its \$1,595 AP4500-E Ethernet access point maintains a rate of 2 Mbps even
at long ranges. In addition, setup and installation is easy. Bay Networks'
\$1,799 BayStack 660 Wireless Access Point can easily be upgraded with
a new PC card. However, all its BayStack 660 documentation is on CD-ROM.

TEXT:

There are a number of reasons why a business might not want to run network
wiring to all computers. The computers may be mobile, or the construction
of the building may not easily accommodate new wiring, or departments might
often need to quickly and easily reconfigure the layout of the office
space. Wireless networks are available to address these issues and others.

Many existing wireless networks were installed to support special
functions, such as in hospitals, stock exchanges, and similar
organizations, where the ability to roam around a building is extremely
important. The first-generation products were typically proprietary, slow,
and expensive.

This is no longer the case-in addition to the OpenAir standard, the
Institute of Electrical and Electronics Engineers has defined the 802.11
standard for interoperability. Speeds have gone from less than 1 Mbps to 2
Mbps under the 802.11 standard, and 11-Mbps data rates are available on
proprietary products and soon under the 802.11 High Rate standard. Pricing
has dropped from more than \$500 to less than \$300.

OpenAir is a standard agreed to by about 40 vendors who were tired of
waiting for the 802.11 standard to be developed. It offers some degree of
interoperability between products from different vendors. Although many
current installations use OpenAir products, with the ratification of the
IEEE standard, it is likely to become much less prevalent.

IEEE 802.11, first defined in 1997, specifies three types of wireless
LANs: diffused infrared, direct sequence, and frequency-hopping
spread-sequence radio. The radio standards operate at 2.4 GHz and support
speeds up to 2 Mbps. Direct-spectrum and frequency-hopping products are not
compatible with each other.

The IEEE 802.11 Working Group has completed the first iteration of
the 802.11 High Rate specification for 11-Mbps wireless connections, which
should provide 10-Mbps throughput, considering the network overhead. While

RadioLAN has been offering 11-Mbps wireless products for a year or so, most vendors waited for the high-rate specification to be ratified, and should be shipping products based on it in the near future (some may even ship by the time you read this, though too late to be tested for this review).

The intent of this review was not merely to test wireless products but to verify interoperability between vendors using the same version of the 802.11 protocol. I also wanted to test the new fast-rate products, but none were available. I was able to test the RadioLAN 11 Mbps product, which should be similar to 802.11 fast rate.

I received wireless products from four vendors: Aironet Wireless Communications, Bay Networks (Nortel), Lucent Technologies, and RadioLAN. I received a number of different products, but in order to simplify things, I tested only the wireless PC Cards and access points from each vendor. Other components available from some or all vendors are ISA and PCI cards for standard desktop PCs, 10BaseT to wireless transceivers for devices such as printers and bridges to connect network segments over distances of up to 1,000 feet.

The Aironet, Bay Networks, and Lucent products are IEEE 802.11 2.4-GHz direct-sequence spread-spectrum devices. They support 1- and 2-Mbps data rates, which translate to 700-Kbps to 800-Kbps and 1.5-Mbps to 1.6-Mbps effective throughput. The RadioLAN devices use a 5.8-GHz frequency that supports an 11-Mbps data rate, using a proprietary protocol called 10BaseRadio. It is representative of the new 802.11 fast-rate products. Aironet and Lucent have announced fast-rate products; Aironet says its access point will be firmware upgradable to fast rate, although the PC Cards will have to be replaced, while Lucent's design requires the replacement of the PC Card in the access point, which is still less expensive than buying a new access point.

Is there an advantage to sticking to the standards? Yes. All of the 802.11 direct-sequence spread-spectrum cards were able to connect to any of the access points, as long as the service-set identifier was the same. The three products use different default service-set identifiers, but setting them to a single one is easy. This means that a company could standardize on either direct sequence or frequency hopping and be confident that products from any of the 802.11 vendors would work in its network, just as different Ethernet network interface cards will work on an Ethernet network.

Setup And Installation

Wireless networks require an access point, which connects the wired network to the wireless segment, with a 10BaseT connection and adapters for the computers. Networks that need to cover a large area can be set up easily-it's simply a matter of adding access points and making sure that all of them use the same service-set identifier. You can also establish different subnets using different service-set identifiers.

A survey of the area to be networked may be necessary to verify adequate signal strength in all areas, depending on the building. A large, open area like a warehouse presents relatively little problem. The ranges noted in the features summary are for typical office buildings-in open areas, the range may be doubled. The utilities available for testing signal strength vary from vendor to vendor.

All the products reviewed include a utility to monitor signal strength. This is useful to identify areas with lower signal strength, which can help pinpoint areas that might require an additional access point. Metal-backed insulation, metal walls (such as corrugated metal shed walls), and heavy metal equipment can degrade the radio signal. Such degradation can be addressed by adding access points.

All the 802.11 products support a peer-to-peer mode, which can be used to exchange data between two stations, whether or not they are within range of an access point.

All the products reviewed are no more difficult to set up than a standard Ethernet PC Card and an Ethernet hub, and because there's no need for cabling, they may actually be easier to install.

Management

All of the access points can be managed via a browser, once an IP address is set using the serial management port. The Lucent access points

have a default IP address set, which means they can be initialized via a browser rather than requiring a serial connection to configure them, and the Radiolan access points can be configured with an IP address via Ethernet using a utility or a wireless PC Card.

Like standard Ethernet hubs and network interface cards, once installed, the access points and PC Cards don't really require much maintenance. Other than creating subnets to reduce the number of users on a given access point, there is little reason that any ongoing management of the access points and cards would be necessary, other than for upgrades of firmware or the like. All vendors offer some level of network upgradability that can broadcast firmware upgrades to multiple access points.

To test the products, I downloaded large files using one, two, and three portables. All the 802.11 cards sustained speeds of about 1.5 Mbps when a single card was in use. When multiple computers were downloading simultaneously, the bandwidth dropped. With two systems, throughput on both systems dropped to about 700 Kbps. With three systems, it dropped to about 440 Kbps on each system. I had only two of the Radiolan cards but observed a similar drop when two were running at full bandwidth at once; throughput when two cards were downloading dropped from 10 Mbps to about 5 Mbps.

The drops in throughput would also happen in a wired network, and, in general, heavy downloads are not characteristic of most network use; in most cases, little degradation in network performance would occur, even with up to 100 users. The more important issue is that the quoted data rates are for raw data, including network protocols. The actual throughput is somewhat less.

While I was unable to test the networks with more than a few PC Cards, I used the Radiolan product at Novell's BrainShare '99 conference a few months ago. With access points positioned all over the convention center, more than 100 users were able to access the network at full Ethernet speeds at all times. I was unable to find anywhere inside the building where I was unable to access the network, and it even worked quite a ways outside, providing access at speeds not noticeably slower than standard Ethernet. This bodes well for the new fast-rate 802.11 products.

In addition to testing throughput, I tested all cards with all the access points. I found that the three 802.11 cards were able to function with any of the access points. While it's impossible to say that all 802.11 products would behave as nicely, it is an encouraging improvement over early 802.11 devices that would work only with their own access points or maybe a few others.

I also tested for range. While I don't have a large office building to roam in, I did take the portables to various places around my home office, both in the office, up the hill to my house, and behind the house to my deck. The distance to the deck was about 200 feet, and even the Radiolan device, rated at 120 feet in an office environment, had no trouble at that distance.

As a worker in a home office, I can testify that it's a liberating experience to plug a wireless PC Card into a portable and be able to access the network from anywhere on the grounds. It's also nice to be able to roam around the house, taking inventory on a portable, without worrying about wires, or to be working in one place, put the portable on standby, move to another location, and resume working, with complete network access.

For administrators who want to get going now and who don't think they'll need more than 2 Mbps, the 802.11 products are stable, interoperable, and easy to set up. The buying decision can be made based on pricing and management functions. For users looking forward to the 802.11 fast-rate products, the Radiolan offering is typical of what they should be like in a couple of ways-they're a lot faster and have a more limited range (120 feet rather than 300+ in an office-building environment). The vendors I spoke with said their fast-rate products will have the same unobtrusive antennas as existing 802.11 products rather than the bulkier antennas used on the Radiolan products.

Administrators who want to implement wireless now, rather than after the end of the summer when the fast-rate specification has been ratified, may want to look at Lucent's products.

It is shipping FCC-approved 11-Mbps products that Lucent says will be

flash-upgradable to the 802.11 fast-rate spec once the standard is set. The access point will also accommodate both standard and fast-rate cards, and be less expensive than the other 802.11 access points. The Bay Networks access point can also be upgraded by adding a new fast-rate card, which should also support the slower data rates, while the RadioLAN access point will be more difficult to upgrade because it will have to be taken apart to replace the radio hardware.

Given the initial problems with interoperability that occurred when the 802.11 specification was first finished, administrators may also wish to take a long look at the RadioLAN products. Though they are not 802.11 and won't be, they have the definite advantage of having been shipping for a year or more.

Aironet

I tested the PC 4500 wireless LAN adapter and AP4500-E Ethernet access point. Setup and installation couldn't be easier. In fact, with a single access point, installation is completely plug-and-play-unpack the access point, attach the antenna, plug it into power and a 10BaseT port, and it's up and running. The access point also supports thin and thick Ethernet (10Base2 and 10Base5).

Getting the PC Cards installed is a matter of plugging them in, inserting the diskette when prompted, and then rebooting. The PC Cards come with a snap-on, small antenna that extends about an inch beyond the side of the portable. Optional extended-range antennas are available. To go beyond the basics, the PC Card can be configured using the network control panel.

To configure the access point, you must use a serial terminal connection, at least the first time. After that, you can assign an IP address, and, from that point forward, administer the access point with a browser. However, configuration is simple and straightforward, and using the serial terminal is not difficult-the advantages to the browser-based configuration utility are the graphical user interface and the ability to manage configurations remotely from anywhere on the network.

Bay Networks

Bay Networks offers two product lines, the 650 and 660. The 650 is a frequency-hopping system, and the 660 is direct sequence. I received the Bay Networks BayStack 660 Wireless PC Card and access point. The 660 access point is a relatively small unit with both 10BaseT and coaxial (10Base2) connectors. Rather than having a built-in radio interface, it uses the same PC Card as portable computers. This allows a relatively inexpensive upgrade to 802.11 fast rate when it's available. The 660 devices are rated at up to 300 feet in enclosed places or up to 2,000 feet in open areas.

The documentation for the Bay Networks products was supplied only on CD-ROM, other than a short booklet that didn't even have much quick-start information. The documentation is clear, thorough, and complete, but like many administrators, I prefer printed documentation. You never know whether you'll have a system with Adobe Acrobat on it around when you need it, and installing Acrobat from the CD and then reading the documentation takes a lot longer than digging out the manual. You can print the Acrobat files, but it's a cumbersome process at best.

As with the other products, installation was very simple and went smoothly. The BayStack manager has more stringent requirements (version 4.0 or higher of Netscape Navigator or Microsoft Internet Explorer, Java Runtime Engine 1.1.4 or higher), but has a nice GUI interface and can automatically **discover access points**, eliminating the necessity for configuration via a serial interface.

Lucent

The Lucent WaveLAN has a number of intriguing features. The access point has two PC Card slots, and uses the same PC Cards as portables. This is also true of the Bay Networks access point, but the Lucent device, with two cards, can support both a standard 802.11 card and a fast-rate card, allowing an easier migration to the higher data rates, or allowing both to be supported if some systems need faster rates than others. Alternatively, it can support two separate overlapping networks. Each of the two radio cards can support approximately 100 users.

The PC Cards have an antenna that is slightly larger than the Aironet and BayStack cards, though it does support a longer range and also supports

an optional extended-range external antenna, which extends the range by about 15%, from 550 feet at 2 Mbps to 630 feet. The cards can also be set to attach to any available access point or to a specific one.

The WaveManager/Client tool is installed in a notebook computer with a WaveLAN PC Card. It can visually show all the access points within reach of the mobile station and the quality of the links between the mobile station and each of the access points. It can monitor several access points simultaneously, reducing the time required to perform a site survey for determining the placement of access points, and it can also be used to perform post-installation verification of full building coverage. A log function makes monitoring over a longer period of time more convenient.

RadioLAN

RadioLAN uses a proprietary protocol running at 5.8 GHz, rather than the 802.11 standard of 2.4 GHz used by the other products. This means that it can't be upgraded to 802.11 fast rate. However, it has the advantage of about a year of refinement at the 11-Mbps data rate.

I received two different PC Cards, models 130 and 140, as well as the model 208 BackboneLink access point. The CardLink 130 uses a fairly large separate antenna module, and the MobileLink 140 uses a much smaller attached antenna. They both offer the same 120-foot range, but the 140 is more expensive. The access unit uses the same antenna as the model 130 PC Card, easing inventory headaches.

The CardLink's separate antenna is intended to be mounted on the back of a portable, using either a permanent mount or a Velcro mount. The antenna and the cable to the PC Card can be cumbersome. The 140 has a smaller attached antenna that is hinged so it can lay flat when not in the portable. The antenna is raised to a 90-degree angle when it's in use. It is much less cumbersome, although still bulkier than the slower 802.11 units.

The access point can be configured through Ethernet, using a PC and a configuration utility or via the wireless network, in addition to the usual serial terminal connection. Many administrators will appreciate not needing to dig up a serial cable and get the serial terminal to work before being able to configure the access points.

The access points include Web software for updates, which allows upgrading all access points via flash technology.

At A Glance

Aironet

Aironet Wireless Communications

Akron, Ohio

800-247-6638

www.aironet.com

Price: \$495 for card, \$1,595 for access point

Strengths

- Simple setup and installation
- Good range; maintained 2 Mbps even at long ranges

Weakness

- None

At A Glance

BayStack 660 Wireless Access Point

BayStack 660 PC Cards

Bay Networks

Santa Clara, Calif.

800-822-9638

www.nortelnetworks.com

Price: \$509 for card, \$1,799 for access point

Strength

- Access point is easily upgradable with a new PC card

Weakness

Documentation is supplied only

on CD-ROM

At A Glance

WaveLAN

Lucent Technologies

Murray Hill, N.J.

800-928-3526

www.wavelan.com

Price

\$295 for 2-Mbps WaveLAN/IEEE PC Card, \$495 for 11-Mbps high-speed WaveLAN/IEEE Turbo PC Card, \$1,295 for WavePoint Access point, \$70 for antenna

Strengths

- Very good setup and management utilities
- Long range
- Dual PC Cards in access points allow network to support more users or both regular and fast cards at once
- PC Card allows use of additional antenna without removal of standard antenna

Weakness

- Access point is relatively expensive

At A Glance

MobileLink Model 140

RadioLAN

Sunnyvale, Calif.

408-616-6300

www.radiolan.com

Price: \$449

Strengths

- High speed-can sustain 10 Mbps
- Excellent documentation
- Model 140 has small antenna, low power consumption

Weakness

- Relatively bulky antenna compared with 802.11 units

Copyright [copyright] 1999 CMP Media Inc.

COPYRIGHT 1999 CMP Publications, Inc.

COPYRIGHT 1999 Gale Group

PUBLISHER NAME: CMP Publications, Inc.

COMPANY NAMES: *Lucent Technologies Inc.; Aironet Wireless Communications Inc.; Bay Networks Inc.; RadioLAN Inc.

EVENT NAMES: *350 (Product standards, safety, & recalls)

GEOGRAPHIC NAMES: *1USA (United States)

PRODUCT NAMES: *3662116 (Wireless Local Area Networks); 3662100

(Communications Equipment ex Broadcast); 3661257 (LAN/WAN Adapters)

INDUSTRY NAMES: BUSN (Any type of business); CMPT (Computers and Office Automation); TELC (Telecommunications)

NAICS CODES: 33422 (Radio and Television Broadcasting and Wireless Communications Equipment Manufacturing); 33429 (Other Communications Equipment Manufacturing); 33421 (Telephone Apparatus Manufacturing)

TRADE NAMES: Aironet Wireless Communications PC4500 (Wireless LAN/WAN adapter); Bay Networks BayStack 660 Wireless PC Card (Wireless LAN/WAN adapter); Lucent Technologies WaveLAN (Wireless LAN/WAN adapter); RadioLAN CardLink 130 (Wireless LAN/WAN adapter); RadioLAN MobileLink 140 (Wireless LAN/WAN adapter); Bay Networks BayStack 660 Wireless Access Point (Wireless LAN/WAN bridge/router); Lucent Technologies WavePoint II Access Point (Wireless LAN/WAN bridge/router); Aironet Wireless Communications AP4500-E (Wireless LAN/WAN bridge/router)

SPECIAL FEATURES: COMPANY

13/9/11 (Item 1 from file: 624)

DIALOG(R) File 624: McGraw-Hill Publications

(c) 2005 McGraw-Hill Co. Inc. All rts. reserv.

00877433

Computerizing patient education documents: Here's a way to clean out those files!

JERRY F. POTTS, MD

Postgraduate Medicine, Vol. 102, No. 2, Pg 39

August 1997

JOURNAL CODE: PGM

TEXT:

In the March 1997 column, I outlined our clinic's attempt to move to an electronic medical record, which has been a slow and somewhat painful process. As a result of a grant from a local neighborhood group, we have also been concentrating on another project--to somehow computerize patient education handouts.

Problems getting handouts to patients

Many primary care clinics try to educate patients regarding various aspects of their disease. Certainly, informed patients are more able to recognize problems when they occur and to find suitable care when it is needed.

Unfortunately, during a busy clinic day, physicians often overlook or rush through the patient education aspect of care. That's why the most successful programs rely on some system for determining the need for and providing patient information that is structured into the clinic visit and does not depend entirely on the physician.

Many clinics have a formal discharge process that allows nurses or other personnel (eg, social workers, diabetes educators, dietitians) to instruct patients as part of the clinic visit. In some cases, the physician makes a note of what is needed and someone else gives the educational material to the patient.

Problems keeping copies on hand

Finding the material can be another problem. Traditionally, patient education handouts are filed in a central location and handed to patients when they are discharged. Problems with this system include out-of-date material, unreadable photocopies, inadequate supplies of handouts on common topics, and ``creative'' filing systems that frustrate those trying to quickly locate the proper material for patients who typically want to get out the door.

Allowing a computer to take over the function is often the answer to these problems. Putting all patient education handouts in a simple database that can be used by all clinic personnel quickly does away with ``I can't read this,'' ``We're out of that one,'' and ``I wonder where that one disappeared to.'' In addition, all the file space used previously is freed up, since handouts are ``stored'' in the computer and printed out only as needed.

Our plan to solve delivery problems

In our project, we attempted to move delivery of educational materials one step closer to the patient encounter. Clinic personnel were surveyed for their thoughts on the process, and we decided to let nurses select what handout was needed while they were still in the exam room with the patient. Nurses would have access to available handouts with a small handheld computing device; they'd select the one to be printed, and it would be ready for patients to pick up as they left the office.

We certainly did not have the needed expertise to put together such a complicated effort, so we approached a software firm in Minneapolis (Business Brothers, 612-853-3024) for their help in project development. We chose to work with Macintosh computers, since Macs and the handheld Newton 120 PDA (Personal Digital Assistant) produced the right combination of software and hardware for our project. After defining our needs (eg, number and types of devices, costs), developers put together software to run the system.

The hardware side of the system includes two Dayna `` wireless access points ,'' two LaserJet 4M printers, and a Mac 7200/100 (with an attached 600-dpi full-page scanner) wired together into a small Ethernet network. Each of the three PDAs has a Dayna wireless communication card in the PCMCIA slot. The Mac was set up as both the server for the system and the scanning workstation. The scanning software saves each scan as a postscript (.ps) file (200 to 300 K per page), which is stored with up to 10 key words in a 4th Dimension database application (available through ACI US, 800-881-3466, or on the Web at www.acius.com).

The Mac also works as a server for the wireless side of the system. Two wireless access points were placed far apart in the clinic for maximum coverage. An application runs continuously, scanning the wireless access points for any communication from the PDAs. Each PDA is assigned to one of the printers and is loaded with software that communicates via radio frequency technology to a wireless access point . Each of the wireless access points has an Ethernet connection that is wired to the same network that the Macintosh server is on.

Our plan in action

We scanned several hundred patient education documents in several languages (eg, Spanish, Hmong, Vietnamese) into the system and were ready to go. This is how the system works:

When a nurse wants a handout for a patient, he or she simply writes or types one of the key words for that handout into the PDA. (Handwriting recognition has improved significantly since it was introduced, so it is very simple to use, but there is also a small virtual keyboard that pops up on the screen, and keys can be tapped to ``type'' in key words.) The requested key word travels via radio frequency to the wireless access point , which hands off the request to the Ethernet connection and hence to the Mac. When the system locates the requested key word in the database, all matching document titles are sent back to the PDA. The nurse selects the desired document title, the request is sent back to the Mac, and the desired handout is printed at whichever printer the particular PDA is assigned to.

This may sound like a lot of communication, but all this back-and-forth occurs very quickly. We found that the total time from entering a key word to printing the finished document is less than 90 seconds.

Success with a price

The computerized patient handout system we came up with offers several advantages over a traditional paper filing system and even over other computer-storage systems. The most useful feature is its extreme portability. Because of the location of the wireless access points in the clinic, nurses can carry the PDAs into any exam room or work area and still access the database and print whatever is requested. We don't need to keep any paper copies, and new handouts can easily be added to the system. An important advantage is that each document receives a date of input when it is scanned, providing a useful reminder to review and update old material.

As with any new project, ours had many minor irritations. We were attempting to work with relatively new technologies in a new way. Most wireless applications only send information to a server, with no back-and-forth communication. The type of interaction we wanted made the software much more technical and tougher to put together. Add purchasing delays and personnel issues, and what started out to be a 6-week project took about 6 months. Being on the cutting edge can be painful!

Simpler ways to get handouts by computer

A quick and relatively painless way to access computer-based patient education information is through the World Wide Web. Several Web sites have extensive patient education libraries online (try www.vh.org/Patients/Patients.html or www.aafp.org/patientinfo). By having your browser up and running and pointed to one of these sites, you can do a quick key word search and bring the desired document up on the screen for printing. Disadvantages of such a system are that you are limited to topics that are already online and you cannot modify or add handouts.

Obtaining a disk or CD-ROM with patient education handouts ready to go is an even easier approach. For example, for about \$100, members of the American Academy of Family Physicians can buy a CD-ROM with English and Spanish text on nearly 200 problems typically seen in a family practice or primary care clinic through CMC Research Inc (503-242-2567; E-mail address, cmcresrch@aol.com; Web site, www.cmcresearch.com).

You may have a method of your own that works well or you may have no problems at all with your paper filing system, and that's great. It doesn't really matter how delivery is accomplished, just so it is. Patients clearly benefit from having a handout to refer to after they leave the clinic.

Copyright 1997 The McGraw-Hill Companies, Inc.

COMPANY NAMES: American Academy of Family Physicians ; Business Brothers ;
CMC Research Inc

13/9/16 (Item 4 from file: 647)
DIALOG(R)File 647:CMP Computer Fulltext
(c) 2005 CMP Media, LLC. All rights reserved.

01219185 CMP ACCESSION NUMBER: NWC20000710S0019
Cisco Aironet Beats Rivals-With Ease - While Cisco's 340 Series rides its friendly features to the top, Lucent Technologies' Orinoco solution nabs our award as the best value in 802.11b networking.

Joel Conover
NETWORK COMPUTING, 2000, n 1113, PG98
PUBLICATION DATE: 000710
JOURNAL CODE: NWC LANGUAGE: English
RECORD TYPE: Fulltext
SECTION HEADING: Reviews - 802.11b
WORD COUNT: 3997
TEXT:

Cisco Systems Cisco Aironet 340 Series

Network Computing Editor's Choice

Grade: A-

The Cisco Aironet 340 Series earns our Editor's Choice award because of the wireless hardware's top-notch performance, ease of installation and overall ease of use in our lab tests. Likewise, the Cisco Aironet 340 Series Access Point (AIR-AP342E2C) packs a lot of features and functionality into a very small package. The Cisco access point has features that simplify deployment, and it includes all the functionality an enterprise needs to fine-tune a wireless network. The clear and concise management interface is a dream for both novice wireless users and advanced power users. The interface, which can be accessed via a serial port, telnet or a Web interface, is aware of multiple access points in the network and capable of managing a cluster of wireless access - point devices as a managed group. However, Cisco-and the industry in general-has a long, long way to go to make managing an enterprise of wireless devices less of a headache.

The Cisco Aironet 340 Series PC Card (AIR-PCM342) is well-designed; its solid single-piece construction is rugged and durable. The access point-PC Card combo outperformed every vendor's solution by at least 15 percent in raw throughput tests. The 340 Series PC Card has a 5-volt design. Cisco's product sits in the middle of the pack in terms of power consumption. Its power-saving mode delivers excellent throughput, but the unit's 500-milliwatt quiescent power draw drops it to fifth in our power-consumption tests. The 340 Series' strong showing was gained through proprietary (though interoperable) performance extensions. Our ongoing lab tests have shown that Cisco products don't soar nearly as high when non-Cisco PC Cards are used with Cisco access points.

The Aironet family of products seems to be aimed primarily at Wintel PC users; no support for Microsoft Windows CE or Apple Computer Macintosh was available during our tests. In addition, Cisco charges the most for its units, demanding a hefty \$249 per PC Card. The Cisco tax strikes once again. Pricing is an interesting game in this market, however. For example, Lucent Technologies sells its access point for \$1,000 but also requires the purchase of a wireless PC Card to put in the access point. Likewise, Cisco charges additional fees for antenna diversity and encryption, even though these options are "software upgrades." And all this is calculated without discounts the vendor may offer.

Cisco's PCI-based adapter is simply a PC Card mounted on a PCI-based PCMCIA host adapter. Most vendors take this approach, and even those that don't (such as Compaq Computer Corp., with its WL200 11 Mbps Wireless LAN PCI Card) still identify the PCI card as a "PCMCIA bridge device." These PCMCIA-on-a-stick solutions work just as well as their PC Card brethren. The vendors making these PCI and ISA solutions are trading off design time for cost of deliverables. That is, does the vendor sell enough PCI and ISA cards to justify creating a lower-cost, integrated design? The answer, it appears, is no. None of the vendors participating provided an ISA or PCI adapter that didn't eventually present a PCMCIA bus to the host-proof that wireless LAN is still aimed primarily at mobile applications.

The 340 Series Access Point is a breeze to use. In terms of management features, this little package has it all, offering options for telnet, Web-based management and serial-based configuration. The hardware is easily mountable. Cisco supplies all the hardware for a professional installation at your business. We had no problems getting this unit up and running. Unfortunately, the hardware affords no place on which to attach external antennae; its dual diversity antennae are permanently affixed to the access point. Cisco didn't provide us with its detachable-antenna model. We had no problems roaming our call center using a single **wireless access point**.

The access point and PC Cards support 40- or 128-bit encryption. These features are configurable by a license key, which must be bought with the features in mind-that is, you pay only for what you need but don't get the flexibility of everything at a single price.

Cisco Aironet 340 Series Access Point (AIR-AP342E2C), \$1,299; Cisco Aironet 340 Series PCI Adapter (AIR-PCI342), \$349; Cisco Aironet 340 Series PC Card (AIR-PCM342), \$249, Cisco Systems, (800) 326-1941, (408) 526-4000; fax (408) 526-4100. www.cisco.com

Enterasys Networks RoamAbout Solution

Grade: A-

Tied for second place with Lucent's Orinoco, Enterasys Networks' RoamAbout 6.0 Access Point is a powerful wireless solution. Like Cisco's

solution, the RoamAbout access point is built with the enterprise user in mind. A serial port can be used to configure the access point initially. Once the unit has been configured, remote configuration is supported via telnet or the provided SNMP utility.

The RoamAbout is one of the most feature-rich access points we tested. The hardware has support for power over Ethernet, which is accomplished by using spare pairs in the Category 5 cable. This greatly simplifies installation in locations where power is not readily available. But you need to be careful with this technology, too: It isn't particularly intelligent, and it most certainly cannot be run through a repeater or a switch. Power over Ethernet is a sort of last-mile power and wire solution designed to simplify wireless installations.

Furthermore, the RoamAbout is the only product we tested that lets you use the remote-power feature as a redundant power source, enabling truly mission-critical wireless networks.

The Enterasys access point uses a PC Card adapter to provide wireless-radio functionality. Thus, as the industry progresses, you can upgrade the wireless radio to the latest technology—a feature shared with products from Lucent and Intermecc Technologies. The access point allows a high degree of wireless LAN configurability.

Unlike the PC Cards, the Enterasys access point is not an OEM product. The access point is robust and includes serial and host-based management features, as well as telnet access. Still, like most of the solutions we tested, Enterasys' RoamAbout lacks a complete management package tailored to dozens or hundreds of access points and users.

Enterasys resells the wireless Orinoco PC Card to deliver wireless connectivity both to the access point and to the PC. Like the Lucent card, Enterasys' product delivers performance well above average, and its power consumption and range were among the best we tested.

RoamAbout 6.0 Access Point, \$999; 40-bit Encrypt card, \$199; 128-bit Encrypt card, \$249, Enterasys Networks, (603) 332-9400; fax (603) 337-2211. www.enterasys.com/wireless or sales@enterasys.com

Lucent Technologies Orinoco Wireless Networking System for Enterprise

Network Computing Best Value

Grade: A-

Lucent's Orinoco Wireless Networking System for Enterprise earns Network Computing's Best Value award by lowering the bar on wireless pricing. At \$179 for Orinoco PC Cards, Lucent's solution costs \$20 per card less than its closest competitor and represents a phenomenal improvement over the \$500 to \$800 per-unit pricing of just a year ago. Lucent's Orinoco PC Card has an integrated antenna; however, it also sports a small accessory connector that can accept an external wireless antenna. Lucent's and Enterasys' solutions were second to Cisco's by a very thin margin. The ease of management and raw performance provided by the Aironet 340 Series gave it a slight edge over Lucent's Orinoco.

Orinoco is a 5-volt PC Card. Lucent provides drivers for almost every operating system, including all flavors of Microsoft Windows, Windows CE, DOS, Linux and Apple MacOS. The Lucent solution is the most widely supported adapter of all the units we tested, a boon for sites with multiple operating systems to support. Lucent's Orinoco took second place in our performance tests, with an average of 4.5 Mbps of throughput and a top throughput of 4.9 Mbps. Orinoco's power utilization under standard operating conditions was the lowest of all the 5-volt cards we tested;

when we enabled power-saving mode, it performed extremely well, using only 75 milliwatts of power in quiescent mode, the second lowest of all the products we tested.

The Lucent Orinoco access point features a dual-slot PCMCIA design. This design, Lucent claims, gives you a number of options, including migration from previous wireless technology/standards or, alternatively, a way to improve performance or fault tolerance within a single cell. The access point takes the same Orinoco cards that are installed in notebook computers. It can also be a wireless bridge (building to building) with the extra slot.

The Orinoco access-point management software is functional, but not fantastic. Lucent has been using the same wireless-access configuration software for years; it **discovers access points** on the network and then lets you configure most of the operational parameters on a per-access-point basis.

Basic access-point features as well as specific wireless parameters are configurable from a single interface. However, only one access point can be managed at a time.

The Orinoco access point checks in at under \$1,000. However, Lucent hides some of the cost of its solution in packaging. The Orinoco access point does not come with a wireless PC Card. You must purchase the PC Card separately, putting the cost near \$1,200.

Orinoco Wireless Networking System for Enterprise, \$995 for WavePoint II access points, \$179 for Orinoco PCMCIA cards, Lucent Technologies, (800) WAVELAN, (973) 581-4297; fax (973) 581-3223. www.wavelan.com or vonschaumbur@lucent.com

3Com Corp. 3Com AirConnect 11 Mbps Wireless LAN

Grade: B+

3Com's AirConnect 11 Mbps Wireless LAN product is a pleasure to use. The AirConnect PC Card we received came in a starter pack, which includes three of the wireless PC Cards and a **wireless access point** for just under \$1,800. The AirConnect PC Card is actually an OEM unit from Symbol Technologies. The card features a modular detachable-antenna design. We speculate that excessive wear on the antenna/main body could damage the delicate hinge between the wireless PC Card and the antenna. If you're looking for extra range, you can remove the modular antenna and instead attach an external special-purpose antenna.

In our tests, the 3Com wireless PC Card performed admirably, coming in just behind Lucent's and Cisco's products, with a peak throughput of 4.6 Mbps and an average of about 4 Mbps.

The 3Com client is one of the best we tested; it includes support for Mobile IP, which lets you roam among multiple subnets, a handy feature in a typical, routed enterprise infrastructure. 3Com is also the only vendor that let us specifically choose an access point, rather than having the software just pick the strongest access point. This flexibility is a valuable feature if you are trying to manually segregate your traffic to balance network load. Although it's tedious to configure mobile users, once configured, they can roam just as other users can. You can also automate the process by forcing the user to join a particular network area using the 802.11b ESSID (Extended Service Set ID) field. We still wish there were a better way of associating users to access points.

The 3Com access point boasts a large fixed-configuration antenna. Upon closer inspection, we found the access point actually contains a PC Card radio with a special antenna fixed to the PC Card. That card does not

appear to be removable.

Configuration and monitoring tools on the 3Com access point are extremely flexible and a snap to use. Like Enterasys' RoamAbout, AirConnect also supports a power-over-Ethernet technology, which lets you place the access point anywhere you can place an Ethernet port. You can manage the 3Com access point from a serial connection, telnet or Web interface. The management interface also lets you manage multiple access-point configurations from a single access point. You can save a configuration or update firmware from one access point to all access points on your network (Cisco's Aironet also supports this feature). We found this feature to be potentially useful but a bit buggy when it came to firmware upgrades. We hope 3Com will work these bugs out in a future code release. Unreliable code is worse than not having the feature at all.

3Com AirConnect 11 Mbps Wireless LAN, starts at \$1,795 for the starter pack of one access point and three PC Cards, 3Com Corp., (800) NET-3COM, (408) 326-5000; fax (408) 326-5001. www.3com.com

Intermec Technologies Intermec 2101 Universal Office Access Point Solution

Grade: B

Intermec provided us with a unique wireless solution that includes its Intermec 2101 Universal Office Access Point and a 3.3-volt Orinoco PC Card. Intermec's hardware relies on external antennae, which have advantages and disadvantages. Having an external antenna on a wireless PC Card offers the opportunity for extended range and performance, but it also requires a small wire to run from the PC Card to the external antenna. In a typical environment, the external wire is both cumbersome and prone to damage. We see the Intermec solution being used primarily in applications in which users are not mobile but require wireless technology to provide connectivity.

The Intermec wireless access point is a two-port PCMCIA-based wireless solution, in some ways similar to Lucent's Orinoco wireless access point. Like the wireless PC Cards in the workstations, however, Intermec uses external antennae for its access-point product. The Intermec wireless access - point product is easier to configure than the Lucent product; the 2101 features a serial port and telnet and Web-based interfaces to configure and manage the device. However, Intermec's access point is almost twice as expensive as the other products in this review. Historically, Intermec has delivered rugged products designed for outdoor use. However, this access point has a simple plastic design, certainly not suited for the industrial applications at which it seems to be aimed.

Intermec's performance was very middle of the road, with average throughput of around 4 Mbps. On the positive side, the wireless client had the lowest quiescent power utilization-only 53 milliwatts.

Intermec 2101 Universal Office Access Point, \$2,090; Intermec 2102 Access Point, \$950; Intermec 2126 PC Card, \$229, Intermec Technologies, (800) 347-2636, (425) 348-2600; fax (425) 355-955. www.intermec.com or info@intermec.com

Compaq Computer Corp. WL100, WL200, WL300, WL400 Wireless LAN Solution

Grade: B

Compaq presented us with a complete wireless networking solution that included access points, PC Cards, PCI cards for desktop systems and a unique software wireless access point. Compaq's package appeared to have all the right pieces, but the performance and range just weren't

there.

Compaq's wireless PC Card is 3.3 volts and is manufactured by Intersil Corp. In our tests, the Compaq card had the lowest overall performance. In our call-center range tests, the wireless signal dropped off almost completely at the center of our coverage area. Whether this is the fault of drivers, antennae, access points or the PC Card itself, we were unsure. Compaq lauded the card as having superior 3.3-volt technology, citing the way it integrates with the end-to-end solution, including Compaq's handheld personal organizer. In our tests, the 3.3-volt card did use far less power than some devices, but its power utilization was mediocre-759 milliwatts during quiescent operation with power saving enabled.

Compaq's access point is a NoWires Needed OEM product. The access point is manageable only via the NoWires Needed management software, which-as we mention below-isn't particularly user friendly. The access point is a fixed-configuration device, with no removable (PCMCIA) radios.

One impressive product in the Compaq solution is the software access point. Rather than spending upward of \$1,000 per access point, you can turn any spare PC into a fully functional access point with this software. Using Compaq's WL200 11 Mbps Wireless LAN PCI Card, you can build a **wireless access point** for less than \$325 (compared with \$899 for the hardware access point). The **wireless access - point** software can significantly lower the total cost of ownership of a wireless solution and can be an ideal SOHO solution, given that every PCI NIC is bundled with a standard-license edition of Deerfield.com's WinGate, which is a popular NAT (Network Address Translation) and proxy software package. Our tests showed the software access point is just as functional as a hardware-based access point in terms of performance and interoperability.

WL400 11 Mbps Wireless LAN Hardware Access Point, \$899; WL100 11 Mbps Wireless LAN PC Card, \$199; WL200 11 Mbps Wireless LAN PCI Card, \$199; WL300 11 Mbps Wireless LAN Software Access Point, \$125, Compaq Computer Corp., (800) 345-1518; fax (281) 518-1442. www.compaq.com

The NoWires Needed 11 Mbps Wireless LAN

Grade: B

The NoWires Needed 11 Mbps Wireless LAN solution we tested was an early beta. During the course of our tests, the company was purchased by Intersil (the company that makes the Prism chipset). NoWires Needed is an OEM provider of wireless equipment for several of the LAN wireless vendors, including BreezeCom and Compaq. However, the equipment we tested was a different generation and model than the OEM equipment the company provides to other vendors.

The 5-volt wireless PC Card provided by NoWires Needed has a fixed-antenna construction. In our lab tests, the NoWires Needed card turned in the best encrypted performance-it was the only card to come in above 5 Mbps with encryption enabled. Furthermore, this card has great power-utilization statistics. The NoWires Needed product doesn't have a power-saving "mode"-it always operates in power saving. Power consumption in quiescent mode was about 150 milliwatts-lower than many of the competitors' results in power-saving mode.

The NoWires Needed driver suite is a bit sparse in terms of diagnostic tools. However, NoWires Needed took the extra effort to provide highly visible encryption warnings and information, a detail the other vendors overlooked.

The NoWires Needed access point is small but effective. Integral to the NoWires Needed solution are the options for 40-bit or 128-bit

encryption, or NoWires Needed's own 128-bit AirLock security. A public /private key exchange system that eliminates the need for distributing shared keys in an encrypted environment, AirLock is an unusual and innovative feature that takes wireless security to a new level. Of course, AirLock is proprietary, and it prevents people only from "sniffing" your wireless data from the air. AirLock's key negotiation eliminates one aspect of security by not requiring the user to enter a public key. We think the trade-off of keyless security is well worth the lack of public keys. Fortunately, NoWires Needed hasn't ignored the need for standards-based encryption. If AirLock isn't available, the client will drop back to standard 40-bit or 128-bit encryption as the environment provides.

NoWires Needed provides management software to configure and monitor access points. However, we weren't impressed by the NoWires Needed management tool, which is also used by several NoWires Needed OEMs. The management software keeps its own state, which didn't always match the state of the access point, making management cumbersome. The software often didn't reflect the state of the remote access point, and sometimes changes we made weren't represented on the remote device.

Priced at \$219 for a client PC Card and \$999 for the Enterprise Access Point, the NoWires Needed solution is a solid performer and a good bargain.

NoWires Needed 11 Mbps Wireless LAN, \$219 for PC Card, \$999 for Enterprise Access Point, \$499 for Small Business Access Point, NoWires Needed BV, +31-30-229-60-60, (650) 330-1466. www.nowiresneeded.com or info@wnw.com

Farallon Communications SkyLine 11 Mb Wireless PC Card

Grade: B-

Farallon Communications is yet another vendor offering a wireless 802.11b high-rate PC Card, but the company does not make an access-point product. We recently tested Farallon's 802.11b wireless product on the Macintosh in our Real-World Labs(r) at the University of Wisconsin-Madison (see "Farallon's Faster SkyLine Does Mac and Windows, Too," at www.networkcomputing.com/1112/1112sp4.html). Here we find it again; however, this time the tests focus on the Wintel platform. The Farallon SkyLine 11 Mb Wireless PC Card is an Intersil OEM product, but Farallon has done additional development to provide support for the Mac. Note that this is not the recently acquired NoWires Needed product we cover above, but another (older) Intersil reference design.

In the lab, the Farallon card performed around the top end of average, with a maximum throughput of 4.5 Mbps and an average of around 4.2 Mbps. WEP-encrypted performance was respectable, too, with top throughput exceeding 4 Mbps and average throughput of around 3.8 Mbps.

The Farallon card has an integrated antenna and driver support for MacOS and Windows 95/98 and NT 4. At \$199, Farallon's SkyLine is competitively priced.

SkyLine 11 Mb Wireless PC Card, \$199, Farallon Communications, (800) 613-4954, (510) 346-8000; fax (510) 346-8119. www.farallon.com or info@farallon.com

Zoom Telephonics ZoomAir Wireless Networking

Grade: C+

Zoom Telephonics also provided us with a wireless PC Card. The ZoomAir Wireless Networking card is actually an Intersil OEM product.

Zoom's product matches Lucent's in price, coming in at a low \$179 per card. The ZoomAir is a 5-volt card with a permanently attached antenna. As we mention in "Top 10 Things To Know About Wireless" (see www.networkcomputing.com/1113/1113f2side2.html), the wireless industry is dominated by a small number of hardware manufacturers. The difference in OEM products comes in antenna design as well as driver implementation.

In the lab, ZoomAir's unencrypted performance was on the low end, averaging about 3 Mbps. With encryption enabled, however, the Zoom card zoomed right along, delivering the fourth-best performance of all the products we tested—a solid 4 Mbps.

ZoomAir's installation procedure is meant to be idiot-proof, but it was designed poorly. To install ZoomAir's drivers, you must use the company's setup utility, which installs IP, IPX and NetBEUI protocol support on your operating system whether you want it or not. Of course, you can remove these protocols, but there is no reason the install should unnecessarily add them to your operating system.

Zoom also offers a software access point, but because the company didn't have a PCI card ready in time for our review and provided only two PC Cards, we were unable to test that product in our lab.

ZoomAir Wireless Networking, \$179, Zoom Telephonics, (800) 631-3116, (617) 423-1072; fax (617) 423-3923. www.Zoom.com or sales@zoom.com

BreezeCom DS.11 Wireless Solution

Grade: C+

BreezeCom provided us with its AP-DS.11 Access Point 2.4.0 and SA-DS.11 Station Adapter 2.4.0 solution. Unlike the other vendors, BreezeCom did not provide us with any PC Card adapters. Instead, its station adapter looks like a standard access point but provides Ethernet-to-wireless connectivity to a wireless network, which is just the opposite role that an access point plays.

And unlike some of the other products we tested, BreezeCom's DS.11 solution offered no encryption and no power-saving mode. Then again, because the units must be plugged into the wall, power saving really isn't an issue.

Managing the DS.11 hardware is done from BreezeCom's GUI-driven SNMP manager. Like most of the configuration and monitoring tools we tested, this one was a little clunky. We had a hard time getting it going, but once we figured out the nuances, we were able to configure the hardware appropriately. The performance of the DS.11 was average at around 4 Mbps.

AP-DS.11 Access Point 2.4.0, \$1,195; SA-DS.11 Station Adapter 2.4.0, \$795, BreezeCom, (760) 517-3100; fax (760) 517-3200. www.breezecom.com or sales@breezecom.com

Zcomax Technologies XI-300 11 Mbps Wireless PC Card

Grade: C+

Zcomax Technologies provided us with its XI-300 11 Mbps Wireless PC Card. The Zcomax hardware features a detachable antenna, with a construction similar to that of the 3Com card. Zcomax informed us, however, that it is a top-level hardware provider; that is, it makes its own PC Cards and is an OEM provider to other manufacturers. Power consumption for the XI-300 was much higher than the competition's—1,225 milliwatts in quiescent mode. Performance was average, around 4 Mbps in our client-server tests.

The Zcomax card does not support encryption, so we were unable to test that feature. We spoke with Zcomax about XI-300's power utilization and performance and found out the company is releasing a new driver, but that driver was not available for our tests. The old driver did not have power-saving mode implemented, even though it was an option in the controls; that explains the poor power utilization.

XI-300 11 Mbps Wireless PC Card, \$199, Zcomax Technologies, (562) 926-4588; fax (562) 926-7885. www.zcomax.com or sales@zcomax.com

<http://www.nwc.com/>

Copyright 2000 CMP Media Inc.

COMPANY NAMES (DIALOG GENERATED): Cisco Systems ; Compaq Computer Corp ; Enterasys Networks ; Farallon Communications ; Intermec Technologies ; Intermec 2101 Universal Office ; Intersil Corp ; Lucent Technologies ; Orinoco Wireless ; Network Address Translation ; Network Computing ; NoWires Needed BV ; PC Cards ; PCMCIA ; Real World Labs ; SkyLine ; Small Business Access Point ; Symbol Technologies ; SNMP ; Top 10 Things To Know About Wireless ; University of Wisconsin Madison ; Using Compaq ; Zcomax Technologies XI 300 11 Mbps Wireless ; Zoom Telephonics ; 3Com Corp

?

16/9/2 (Item 2 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2005 The Gale Group. All rts. reserv.

02490297 SUPPLIER NUMBER: 72607065 (THIS IS THE FULL TEXT)
Latest testing and diagnostic products.(Buyers Guide)
Communications News, 38, 3, 28
March, 2001
DOCUMENT TYPE: Buyers Guide ISSN: 0010-3632 LANGUAGE: English
RECORD TYPE: Fulltext
WORD COUNT: 705 LINE COUNT: 00063

TEXT:

Dual-purpose test set
TEST BOTH VOICE AND HIGH-SPEED DATA SERVICES simultaneously with one piece of equipment, saving time and expense. The TS 1200 ADSL/POTS test set is a combination data-safe, butt-in test set and ADSL service tester. Two modes of ADSL testing provide both an automatic test to provide a snapshot of the line, and a manual test that can monitor line conditions for up to 90 minutes. The easy-to-read menu options, digital readouts and graphing capabilities assist technicians in diagnosing problems. Standard features include high-voltage protection, DropSafe and RainSafe technologies, PBX pause, speed dial, last number redial, and tone/pulse dialing.--Harris

www.harris.com

Circle 315 for more information

AUTOMATED FIBER-OPTIC TEST SYSTEM allows the efficient testing of ribbon cables in telecommunications and networking environments. The Ribbon Test System (RTS) performs return- and insertion-loss measurements on terminated fiber-optic ribbon cables, MT-RJ patchcords and other multifiber cables. The system obtains, records and processes measurement data, and generates custom reports. A software package running on a PC-compatible workstation controls the test unit through a GPIB/IEEE-488 interface. The RTS permits the concurrent insertion-loss and return-loss measurements on up to 64 fibers at one time, eliminating the need for time-consuming mandrel wraps. The system can test different cable types simultaneously, and can be customized for specific manufacturing or research applications.--RIFOCS

www.rifocs.com

Circle 313 for more information

TEST THE LATEST DIGITAL WIRELESS FORMATS without replacing costly testing equipment. The 2029 Vector Modulator can turn any analog RF signal generator into a digital signal generator for testing digital wireless products, including base station amplifiers. Coupled with any manufacturer's analog RF signal generator, the 2029 can output digital signals in WCDMA, CDMA2000, IS-95, GSM, IS-136 and EDGE. The unit combines a vector modulator, an arbitrary waveform generator and an RF level-control system. The 2029 supports multiband, multimode phones, and can test 2G, 2.5G and 3G formats, with a frequency range from 800 MHz to 2.51 GHz. The system is able to switch digital formats instantly, and a software upgrade feature enables the 2029 to keep up with changing wireless standards.--IFR Systems

www.ifrsys.com

Circle 312 for more information

Wireless sweeper

EASILY LOCATE ACCESS POINTS and measure coverage in DSSS wireless networks. The Grasshopper is a 2.4 GHz WLAN wireless receiver designed specifically, for sweeping and optimizing LANs. The instrument measures packet error rate, and displays correlated power and total channel power for direct sequence networks that operate on the IEEE 802.11b standard. The Grasshopper detects and differentiates from narrow-band multipath interfaces, such as microwave ovens and frequency-hopping systems, and includes a built-in display, keypad and antenna. The unit features an easy-to-read backlit display to show the received signal strength graphically. The sweeper comes with a rugged, water-resistant carrying case and two removable battery packs.--Berkeley Varitronics

Systems

www.bvsystems.com

Circle 314 for more information

Gigabit Ethernet analysis

GAIN VISIBILITY OF CRITICAL HIGH-SPEED LINKS with a hardware/software system for monitoring, analyzing and reporting network activity. The Gigabit Distributed Vision Suite integrates two Windows-based software packages--Protocol Inspector Version 3.0 and Network Inspector Version 4.1--and distributed hardware analyzers together to maximize effectiveness in locating and correcting network problems at 10/100 Mbps or gigabit speeds. A Network Inspector software module automatically performs network device discovery and trending of port-level traffic on switches and routers, without the expense of outfitting each port. Results can be integrated into reports that may be printed, published to Web pages or passed to Microsoft Visio 2000 for network diagramming. The hardware analyzers feature full-duplex, full-line-rate 10/100 ethernet and new Gigabit Ethernet versions in self-contained rackmounted units. A supplied in-line tap allows nonintrusive monitoring on fiber or copper links, eliminating the need to break and re-enable network connections each time a network segment is analyzed.--Fluke Networks

www.flukenetworks.com

Circle 311 for more information

COPYRIGHT 2001 Nelson Publishing

GEOGRAPHIC CODES/NAMES: 1USA United States

DESCRIPTORS: Hardware buyers' guide; Electronic test device; Network diagnostic/test equipment

EVENT CODES/NAMES: 330 Product information

PRODUCT/INDUSTRY NAMES: 3825200 (Electronic Test & Measure Eqp); 3661267 (Network Diagnostic/Test Equipment)

SIC CODES: 3825 Instruments to measure electricity; 3661 Telephone and telegraph apparatus

NAICS CODES: 334515 Instrument Manufacturing for Measuring and Testing Electricity and Electrical Signals; 33421 Telephone Apparatus Manufacturing

FILE SEGMENT: CD File 275

16/9/3 (Item 3 from file: 275)

DIALOG(R)File 275:Gale Group Computer DB(TM)

(c) 2005 The Gale Group. All rts. reserv.

02399442 SUPPLIER NUMBER: 62099362 (THIS IS THE FULL TEXT)

802.11 for the Masses.(Technology Information)

Kohlhepp, Robert J.

Network Computing, 182

May 15, 2000

ISSN: 1046-4468

LANGUAGE: English

RECORD TYPE: Fulltext

WORD COUNT: 1634

LINE COUNT: 00129

TEXT:

Proprietary wireless LANs have been around for quite some time, but only now have their interoperability and performance begun to shine. Wireless vendors would like to outfit every office-and even your home-with 802.11b-compliant hardware. And maybe they should: Working without wires has never been so easy.

When constructing a wireless LAN, think about how your users will connect to the corporate network and what coverage area, performance and security are needed. Implementing wireless should not disrupt a user's current network setup, leave him or her disconnected, or open your network to security holes.

In the Beginning

Since the early 1990s, wireless LANs operating in all unlicensed spectra (900 MHz, 2.4 GHz and 5 GHz) have been available on a limited scale. However, because of price, performance and interoperability issues,

they were purchased primarily for vertical applications. We tested these devices and didn't recommend them for very many situations.

In June 1997, the first of the 802.11 standards was approved. It specified the physical and MAC (Media Access Control) layers for interoperable wireless LANs. In the physical standard, options existed for DSSS (direct-sequence spread spectrum), FHSS (frequency-hopping spread spectrum) and diffuse infrared. All wireless devices transmitted at the basic 1-Mbps data rate, and nearly all could also transfer data at the optional 2-Mbps rate. Most vendors opted for the DSSS option-no one implemented infrared.

In July 1998, the IEEE proposed another specification, setting the ground-work for 802.11b. This specification moved forward with only the 2.4-GHz DSSS physical layer (using 11 channels in North America), because most vendors were on that path. The major improvement in the "b" revision is the addition of data transfer rates at 5.5 Mbps and 11 Mbps. Plans are under way for operating in the 5-GHz range and offering data rates up to 54 Mbps. But don't count on those rates any time soon: The dust hasn't settled from the introduction of the 11-Mbps units.

Also part of the 802.11 specification is WEP (Wired Equivalent Privacy), a method of encrypting data using the RC4 algorithm between the client and the access point. WEP not only offers privacy, but also adds authentication by requiring an encryption key for access. Support for WEP was spotty in the original implementation, but most 802.11b products include it. Just be forewarned that enabling WEP may decrease performance in some cases.

Wireless Networking

Wireless LANs are not terribly complicated to design. There are only two components-the access points and the clients. Any client can talk to any other device, including another client. It's just a matter of how you configure your software. In the most basic configuration, clients are put into ad hoc, or computer-to-computer, mode. No access points are involved. You can set up a network in your conference room in a matter of minutes and transfer files between laptops at 11 Mbps.

Once you are configured in ad hoc mode, all the computers in your area should be accessible in the same way they are with a wired LAN-provided they are all on the same channel. If you are having difficulty, keep in mind that some vendors, including Apple Computer, work in ad hoc mode on only a single, unchangeable channel. Ad hoc wireless LANs can be considered a temporary setup that will not get you access to other corporate network resources.

Widening Your Horizons

More commonly, wireless LANs are set up in infrastructure mode. Here, hardware-based access points are scattered throughout your organization and bridge the wireless users onto the existing wired network-think of **access points** as **wireless hubs**. Clients are PCs or other nodes that have been equipped with wireless LAN adapters.

During configuration of the access points, you enter an ESSID (Extended Service Set ID) to define the access point's network name. Your client machines need to be configured to associate with an access point with that ESSID. Some clients allow a wild card in the ESSID configuration. In this mode, they will associate with the strongest access point, regardless of its ESSID. In most cases, it is a good idea to configure the clients with the actual ESSID, rather than a wild card, to prevent them from associating with other access points that may be in the area.

If you have multiple access points on the same subnet of your network, you should give them all the same ESSID. A number of access points configured with the same ESSID form an ESS (Extended Service Set).

Most client packages can measure the signal strength of access points. You can use this information to properly distribute access points in your building. If you have a low signal but don't think you need another access point, a higher-gain antenna may suit you-that is, if your access point provides an external-antenna option.

With multiple access points, clients are free to move seamlessly between access points ("roam"), as long as the ESSID matches. This feature is built into the 802.11 specification. When a client starts losing the

signal with its associated access point, it begins to search the area for a closer access point. Once a new access point is found, the client initiates an association with the new access point and a disassociation from the old one. By properly placing access points through your enterprise, clients can move about without losing access to the network.

Secure It All

Afraid of sending your data over the airwaves? You should be. As mentioned, any client that is configured with a wild-card ESSID will associate with any access point. For example, a competitor who is parked outside your building can turn on a laptop, associate with your wireless network and potentially capture unencrypted data packets. Without security enabled on your wireless network, this kind of espionage could happen easily.

Some vendors, including Lucent Technologies, let you implement a "closed network." In a closed network, a client cannot just scan the area for wireless networks; it must be configured to the desired ESSID and broadcast that information for an access point to respond. Chances are slim that an intruder would be able to guess your network ESSID.

The most basic form of control is much like that of Ethernet switch restrictions. Users are locked down by MAC address. This is a very cumbersome method and requires each access point to be configured with a list of MAC addresses (of client NICs) that are allowed to associate with it. Oddly enough, this is probably the easiest method of access control for wireless right now.

There are many forms of proprietary security that vendors have implemented within their own product lines. If you have stringent security needs, you should investigate a single-vendor solution.

There are solutions shipping or in development, such as RADIUS (Remote Authentication Dial-In User Service), that force authentication by the client and let the access point tap into user databases for user access control.

WEP 'Em Into Shape

WEP adds privacy and authentication to wireless LANs. All data passing between the client and the access point are encrypted using the WEP key. WEP is especially important when you're using products that don't support a closed network.

To set up this encryption, both sides are required to know the WEP key. By keeping the key a secret, others aren't able to tap into your wireless network. However, managing those keys can be a headache.

Most products implement a 64-bit key-40 bits of which are secret (this is why some refer to it as a 40-bit key). The key is installed on the access point, usually in the form of a string of 10 hexadecimal numbers. Then the key must be entered into each client as well. As with all forms of security, the passcodes should be changed frequently.

Send your comments on this article to Robert J. Kohlhepp at rkohlhepp@nwc.com.

GLOSSARY

Ad hoc mode: Wireless clients are configured to talk only to other clients. This method is used for setting up temporary networks between devices where no access point is available.

BSS (Basic Service Set): A wireless setup with only a single access point in an area.

DSSS (direct-sequence spread spectrum): A method by which a spread-spectrum radio moves through the available channels.

Offers higher data rates than FHSS.

802.11: The group of standards ratified by the IEEE that defines the MAC and PHY layers of an interoperable wireless LAN at data rates of 1 Mbps and 2 Mbps. 802.11b is an extension to 802.11 that adds data rates of 5.5 Mbps and 11 Mbps.

ESS (Extended Service Set): A group of access points that have the same service set ID.

ESSID (Extended Service Set ID): A string that indicates access points and clients in a network.

FHSS (frequency-hopping spread spectrum): A method by which a spread-spectrum radio hops almost randomly through the available channels.

FHSS offers lower data rates than DSSS but is less susceptible to interference.

Infrastructure mode: A wireless setup whereby clients are set to talk only to an access point.

WEP (Wired Equivalent Privacy): A specification for encryption between wireless devices to prevent eavesdropping.

WiFi: A branding of 802.11b interoperability given out by the Wireless Ethernet Compatibility Alliance.

<http://www.nwc.com/>

Copyright (copyright) 2000 CMP Media Inc.

COPYRIGHT 2000 CMP Media, Inc.

GEOGRAPHIC CODES/NAMES: 1USA United States

DESCRIPTORS: Wireless LAN/WAN system; Standard; Technology overview;

History of computing

EVENT CODES/NAMES: 331 Product development

PRODUCT/INDUSTRY NAMES: 3662116 (Wireless Local Area Networks)

SIC CODES: 3663 Radio & TV communications equipment

NAICS CODES: 33422 Radio and Television Broadcasting and Wireless

Communications Equipment Manufacturing

FILE SEGMENT: CD File 275

16/9/4 (Item 4 from file: 275)

DIALOG(R)File 275:Gale Group Computer DB(TM)

(c) 2005 The Gale Group. All rts. reserv.

02142324 SUPPLIER NUMBER: 20305229 (THIS IS THE FULL TEXT)

Up to spec. (Aironet Wireless Communications PC3500 PC Card Wireless LAN Adapter and AP3500 Access Point; Breezecom SA-PC Prom PCMCIA adapter and AP-10 Pro Ethernet access point; Raylink Access Point and Raylink PC Card meet IEEE 802.11 standard for wireless LANs) (Brief Article) (Product Announcement)

Daly, Robert

PC Magazine, v17, n4, p42(1)

Feb 24, 1998

DOCUMENT TYPE: Brief Article Product Announcement

ISSN: 0888-8507

LANGUAGE: English RECORD TYPE: Fulltext

WORD COUNT: 473 LINE COUNT: 00040

TEXT:

The IEEE 802.11 standard for wireless LAN conformance has been approved for a little over six months (though not yet ratified). At least three popular wireless LAN vendors already have products that comply with the standard.

The standard opens two new radio-frequency transmissions--2.4-GHz frequency hopping and 2.4-GHz direct sequencing--and it addresses the important issue of interoperability among different wireless LAN vendors.

Currently, Aironet Wireless Communication (800-247-6638, www.aironet.com), Breezecom Wireless Communications (760-431-9880, www.breezecom.com), and Raytheon Wireless Solutions (508-470-9011, www.raylink.com) have products that conform to IEEE 802.11. The three vendors are awaiting ratification of the standard before issuing free firmware upgrades.

Aironet Wireless Communications recently released the 3500 Series, which consists of the \$595 PC3500 PC Card Wireless LAN Adapter and the AP3500 Access Point (\$1,795 for Ethernet and \$2,395 for Token-Ring). The PC3500 is a Type II PCMCIA card with a snap-on antenna that can support throughput speeds of 1 Mbps or 2 Mbps. The adapter also provides a smart scanning function that balances loads between various access points as well as a sleeper function that enables a PC to maintain a network connection while consuming a low level of current.

The AP3500 Access Point comes in Ethernet and Token-Ring versions. An administrator can manage it directly from a terminal connection or remotely via a telnet connection, FTP session, SNMP application, Web browser, or

Window-based utility.

Breezecom's answer to the new IEEE 802.11 standard is the Pro Series of wireless products, which include the \$565 SA-PC Pro PCMCIA adapter and the \$1,495 AP-10 PRO Ethernet access point.

The AP-10 Pro is a mouse-size computer device with four front-panel LEDs that display the unit's power status, wired LAN activity, wireless signal quality, and wireless synchronization. The access point comes with a 10Base-T physical interface and can support throughput of 1 Mbps, 2 Mbps, or 3 Mbps. The unit is configured through a dumb terminal connection.

A leader in frequency-hopping radio technology, Raytheon Wireless solutions checks into the IEEE 802.11 arena with its Raylink family of products. Together, the \$1,495 Raylink Access Point and the \$550 Raylink PC Card provide in-building coverage of 500 feet.

The Raylink PC Card features drivers for Windows 95, Windows NT, Windows for Workgroups, and NetWare. The card has a rotating diversity antenna and a data transfer rate of 2 Mbps.

The Raylink Access Point is a wall- or desktop-mountable unit that can employ a Raylink PC Card or a variety of antennas. The access point comes with a built-in 10Base-T connection and offers 2-Mbps data throughput.

COPYRIGHT 1998 Ziff-Davis Publishing Company

SPECIAL FEATURES: photograph; illustration

COMPANY NAMES: Aironet Wireless Communications Inc.--Product introduction; Breeze Wireless Communications Inc.--Product introduction; Raytheon Wireless Solutions--Product introduction

DESCRIPTORS: Networking Hardware Product Introduction

PRODUCT/INDUSTRY NAMES: 3662116 (Wireless Local Area Networks)

SIC CODES: 3663 Radio & TV communications equipment

TRADE NAMES: Aironet Wireless Communications PC3500 PC Card Wireless Adapter (Wireless LAN/WAN adapter)--Product introduction; Aironet Wireless Communications AP3500 Access Point (Wireless LAN/WAN adapter)--Product introduction; Breeze Wireless Communications SA-PC Pro (Wireless LAN/WAN adapter)--Product introduction; Breeze Wireless Communications AP010 Pro (Wireless LAN/WAN adapter)--Product introduction; Raytheon Raylink Access Point (Wireless LAN/WAN bridge/router)--Product introduction; Raytheon Raylink PC Card (Wireless LAN/WAN adapter)--Product introduction

FILE SEGMENT: CD File 275

16/9/8 (Item 2 from file: 621)

DIALOG(R)File 621:Gale Group New Prod.Annou.(R)

(c) 2005 The Gale Group. All rts. reserv.

02890547 Supplier Number: 74864745 (THIS IS THE FULLTEXT)

Intermec's New MobileLAN Manager Software Speeds Installation, Simplifies Administration of Enterprise Wireless Networks.

Business Wire, p0102

May 22, 2001

Language: English Record Type: Fulltext

Document Type: Newswire; Trade

Word Count: 798

TEXT:

Business/High Tech Editors

EVERETT, Wash.--(BUSINESS WIRE)--May 22, 2001

Intermec Technologies Corp. today announced MobileLAN(TM) manager, a platform-independent network management application that enables IT managers to track, manage and ensure the availability of access points within their wireless networks.

Designed to suit the needs of both beginners and experts in managing wireless networks, MobileLAN manager is an intuitive, scalable software solution that increases network efficiency and tracks new and existing devices on the network with great accuracy. The Java-based application works on Windows, HP-UX, Linux and Solaris platforms, with a familiar look and feel to the user, regardless of the operating system. MobileLAN manager

will be available in the third quarter of this year.

"MobileLAN manager allows IT managers of any experience level to support the mobile workers within their wireless network," said Greg Smith, vice president of Intermec's wireless product division. "We've created a solution that helps IT managers protect their company's technology investment, while taking the headache and guesswork out of everyday management tasks."

MobileLAN manager includes real-time, event-driven monitoring of changes and events within the network. When an Intermec access point is involved in an event or change, it immediately notifies MobileLAN manager and the event is logged within the software. SMTP e-mail notification of network events is also available to IT managers so that they receive an instant alert of any change. The e-mail notification then can be forwarded to pagers or phones outside of the network for even quicker response times. This instant notification system eliminates the need for constant polling of access points for events, thus saving valuable bandwidth and increasing overall network efficiency.

MobileLAN manager continually monitors traffic on the network, watching for abnormal or excessive jumps and surges. If activity on one access point increases significantly, MobileLAN manager notifies the IT manager who can act accordingly, eliminating the need to "babysit" the network. The software also offers administrators an interpretation of raw data collected from the network, with an analysis of what may have caused an increase in traffic. An assessment and potential solution to the problem is offered, and the raw data are always available for analysis by the IT manager.

MobileLAN manager's intuitive interface allows administrators multiple views into the network, displaying devices by IP address, MAC address, system name, system location, or a custom-created name. At any time, users can determine what end-devices are connected to any given access point, or to what access point a specific device is connected, making quick work of troubleshooting and problem isolation within the network. A simple right-click within the MobileLAN manager interface generates a comprehensive status report on an individual access point, the LAN, or the entire enterprise network.

The new software lets administrators build wireless networks quickly and easily. Using an efficient and accurate "discovery" process, MobileLAN Manager automatically recognizes an access point when it is added to the network, then discovers any remaining new access points within the LAN. This focused method is more accurate and bandwidth-efficient compared with previous "subnet ping before SNMP query" methods.

Intermec sets itself apart from networking giants by designing and implementing wireless LANs to enable the mobile worker, with freedom of movement as the number one priority. Because mobile workers must maintain their network connection as they move from building to building, Intermec's MobileLAN product family allows roaming across routers and switches seamlessly -- even in a large-scale enterprise environment. Intermec's solutions work with any IP-based client and do not require client-side modifications.

About Intermec

Intermec Technologies Corp., a UNOVA Inc. (NYSE:UNA) company, is a full system and solution provider for wireless networking technology with more than 15 years of industry leadership in wireless technologies. The company developed the first wireless data collection network and has more than 250,000 wireless and 500,000 wired terminals installed to date. Among these is the ultimate "mission-critical" network, and world's largest wireless LAN, NASA's Kennedy Space Center, covering 47 square miles.

Intermec leads the way in the establishment of 802.11 standards, and was among the first companies to receive Wi-Fi certification for wireless LAN interoperability. The company now has the largest and most diverse product family of Wi-Fi-certified access points and end devices on the market today. Intermec's products and services are used by customers in many industries to improve productivity, quality and responsiveness of business operations, from supply chain management and enterprise resource

planning to field sales and service.

COPYRIGHT 2001 Gale Group

COPYRIGHT 2001 Business Wire

PUBLISHER NAME: Business Wire

COMPANY NAMES: *Intermec Technologies Corp.

GEOGRAPHIC NAMES: *1USA (United States)

PRODUCT NAMES: *3573243 (Barcode Readers)

INDUSTRY NAMES: BUS (Business, General); BUSN (Any type of business)

SIC CODES: 3577 (Computer peripheral equipment, not elsewhere classified)

NAICS CODES: 334119 (Other Computer Peripheral Equipment Manufacturing)

9/9/1 (Item 1 from file: 636)
DIALOG(R) File 636:Gale Group Newsletter DB(TM)
(c) 2005 The Gale Group. All rts. reserv.

04967997 Supplier Number: 73634605 (THIS IS THE FULLTEXT)
Internet Security Systems is first to provide customers with comprehensive wireless network security solutions; ISS delivers software, consulting, education and managed security services offerings to address growing wireless security concerns.

M2 Presswire, pNA

April 25, 2001

Language: English Record Type: Fulltext

Document Type: Newswire; Trade

Word Count: 1127

TEXT:

M2 PRESSWIRE-25 April 2001-ISS: Internet Security Systems is first to provide customers with comprehensive wireless network security solutions; ISS delivers software, consulting, education and managed security services offerings to address growing wireless security concerns (C)1994-2001 M2 COMMUNICATIONS LTD

RDATE:25042001

"Drive by hacking" is fast becoming a reality. It is now possible for intruders to cheaply equip a laptop PC with wireless technology, sit within range and invisibly monitor traffic, access applications, and hijack data flowing over someone else's wireless network.

In response to the growing need for wireless security awareness and protection, Internet Security Systems (ISS) (Nasdaq: ISSX) today unveiled a range of solutions including wireless local area network (WLAN) security software, consulting, education and managed security services aimed at helping customers protect their wireless networks.

The real business benefits of wireless networks -- flexibility for in-office knowledge workers, network installation efficiency, user support cost savings and new revenue opportunities -- have led to a rapid increase in organisations deploying WLANs. According to the Gartner Group, 50 percent of all enterprises in the United States alone will have deployed a WLAN by the end of 2002, an increase from 21 percent at the end of last year. At the same time, the fact that neighbours -- friendly or otherwise -- can easily access WLANs means they need strong protection.

"Most companies have no idea that their networks are wide open to wireless security risks," says Christopher Klaus, Internet Security Systems' founder and chief technology officer. "Employees today are adding their own wireless access points to the backbone of their company's network without the knowledge of their IT and security staffs. With a lack of awareness by the company that an access point has been added and a lack of proper security configuration, these **rogue access points** can become an intruder's dream backdoor into a company's network despite the front door firewall."

Wireless Security Risks

Main wireless security risks include:

1. The unauthorised installation of wireless LAN access points
2. The malicious interception of data as it is sent between wireless computers and access points
3. Attacks launched against wireless access points in order to compromise or deny service (jamming) of a network or to serve as a launching pad for attacking other wired or wireless devices
4. Station-to-station attacks, including file sharing, denial of service and traditional Internet attacks
5. Vulnerability of authorised wireless laptops to attack when they roam to public access points such as airports and hotels

For more information on wireless security risks, see ISS's white paper on wireless security at www.iss.net/wireless.

ISS Wireless Protection Solutions

Until now, most organisations utilising wireless technology could only look to authentication and encryption for security. While these are useful and important technologies, organisations need a more complete

solution that automatically identifies, monitors, detects and responds to wireless security risks and threats.

"Customers need complete solutions that can automatically identify and mitigate WLAN security risks," says Mike Lortz, product manager for ISS security management software solutions. "Our intrusion detection and security assessment products can dramatically improve a company's ability to identify rogue devices and mitigate against other wireless risks. Our SecureU education raises awareness of the specific risks and WLAN security consulting services provide direction and advice ensuring that customers' deployments are secure."

ISS's wireless protection solutions available today include:

- * Security Software Products -- Internet Security Systems released today an X-Press Update for its Internet Scanner software, enabling customers to scan and identify rogue wireless access points on their networks. The X-Force team, ISS's leading security research arm, is currently developing additional security risk definitions for new wireless LAN (WLAN) risks and these will be available as X-Press Updates in the near future. Internet Security Systems' security assessment products and RealSecure intrusion detection system can be used today in WLAN environments to monitor for wireless security threats and protect against known security risks. In the future, ISS will adapt its products as needed to address the unique needs of WLAN security risks.

- * Security Architecture Consulting -- Internet Security Systems' Consulting Solutions Group has integrated its in-depth security knowledge and proven methodology into wireless-specific offerings, including evaluations, penetration testing, design and security policy development. Through these consulting services, organisations can seek help from ISS experts as they assess, integrate, securely design, and configure their WLANs and the surrounding network and security products.

- * SecureU Education Services -- Internet Security Systems has recently added a wireless security seminar to its wide array of SecureU education programmes. This is scheduled to debut during Network+Interop in Las Vegas on May 7. With an introduction by ISS founder Christopher Klaus, this seminar will help organisations better understand the nuances of WLAN security and the defensive techniques that can be used to protect WLANs against security risks.

- * Managed Security Services -- As WLAN protection features are added to ISS security software products, ISS's Managed Security Services will also integrate these capabilities into its remote managed security services offerings, delivering seamless protection capabilities for customers.

For a wireless security white paper as well as more information regarding wireless security and ISS wireless security solutions, please visit ISS online at www.iss.net/wireless.

About Internet Security Systems (ISS)

Internet Security Systems (ISS) is a leading global provider of security management solutions for the Internet, protecting digital assets and ensuring safe and uninterrupted e-business. With its industry-leading intrusion detection and vulnerability assessment, remote managed security services, and strategic consulting and education offerings, ISS is a trusted security provider to more than 8,000 customers worldwide including 21 of the 25 largest US commercial banks and the top ten US telecommunications companies. Founded in 1994, ISS is headquartered in Atlanta, GA, with additional offices throughout North America and international operations in Asia, Australia, Europe, Latin America and the Middle East. For more information on ISS in the United Kingdom and the Republic of Ireland, visit the Internet Security Systems web site at www.iss.net, write to ukinfo@iss.net or call 0800 085 2976.

CONTACT: David Bridson, Internet Security Systems Ltd. Tel: +44 (0)118 959 3800 e-mail: dbridson@iss.net Jane Lee, Dexterity Tel: +44 (0)1273 470199 e-mail: jane.lee@dexterity.co.uk Andrew Smith, Object Marketing Ltd. Tel: +44 (0)20 8762 9292 e-mail: andrews@objectmarketing.com

((M2 Communications Ltd disclaims all liability for information provided within M2 PressWIRE. Data prepared by named party/parties. Further information on M2 PressWIRE can be obtained at

<http://www.presswire.net> on the world wide web. Inquiries to
info@m2.com)).

7/9/1 (Item 1 from file: 275)
DIALOG(R) File 275:Gale Group Computer DB(TM)
(c) 2005 The Gale Group. All rts. reserv.

02528387 SUPPLIER NUMBER: 77101456 (THIS IS THE FULL TEXT)
Wavelink Mobile Manager Takes Command Of Wireless Lans. (Software
Review) (Evaluation)

Molta, Dave
Network Computing, 28
July 9, 2001

DOCUMENT TYPE: Evaluation ISSN: 1046-4468 LANGUAGE: English
RECORD TYPE: Fulltext
WORD COUNT: 1304 LINE COUNT: 00110

TEXT:

If you've been involved in an enterprise deployment of wireless LAN technology, you've probably found that the leading infrastructure vendors provide limited management tools. Of the major players, only Symbol Technologies, with its Wireless Network Management System (WNMS), offers an enterprise-class management solution (see www.nwc.com/1124/1124sp7.html). But not surprisingly, it can manage only Symbol devices.

There's help in another corner: Wavelink Corp., an established player in mobile applications and device management, has developed Wavelink Mobile Manager to assist in deploying, managing and securing enterprise WLANs (wireless LANs). The product accomplishes these goals by managing access-point configuration profiles as well as generating alarms and alerts related to problems on the WLAN. It supports Symbol and Cisco Systems access points as well as those from two Symbol OEMs: Ericsson and Intel. A release scheduled for the third quarter aims to support Agere Systems/Orinoco too.

I tested a beta version of Mobile Manager in our Syracuse University Real World Labs(r) and was impressed with its capabilities. Still a little rough around the edges, the product is certainly worth a look by organizations contemplating the rollout of large-scale WLANs, particularly those that span multiple locations.

Its configuration management features greatly increase the ease with which access points can be deployed and managed. While the bugs in the beta version are significant-enough to defer my enthusiastic recommendation until I see a final release-Wavelink's 30-day demo available on its Web site will let you assess the product for yourself.

Mobile Manager comprises two discrete software components: the administrator console and agents running on WLAN segments. The administrator, which runs on Microsoft Windows 95/98, NT and 2000, acts as the management console, interacting with agents running on each segment on which an access point is installed. Agents communicate with the console over any IP infrastructure, and sessions can be encrypted for added security. Like the console, the agents can run on any recent flavor of Windows or on Linux. For enhanced reliability, mirrored agents can run on a single segment.

I installed the console and a local agent on a Dell Computer Corp. Latitude 600-MHz Pentium notebook running Windows 2000 Server. My test bed consisted of three access points: an Intel Pro/Wireless 2011, a Cisco Aironet 350 and an Aironet 340. Each access point was configured on a nonoverlapping RF channel and attached, along with the Latitude, to a Cisco Catalyst 1900 switch. I set up three other notebooks on the network, running Cisco, Agere/Orinoco and Symbol 802.11 NICs.

Installation was smooth. Once I started the administrator application and connected to the local agent, Mobile Manager began its autodiscovery mode by sniffing the wire for broadcasts from access points. It quickly detected all three access points. Discovering devices is one thing; doing something useful is quite another.

The problems I had with the Intel access point were easy to solve. A bug, expected to be eliminated in the final release, prevented the system from assigning an IP address automatically, so I had to connect to the console port with a serial cable and configure it manually.

Major Subsystems

Mobile Manager includes powerful capabilities targeted at large-scale deployments. First, using a Windows Explorer-like hierarchical interface, Mobile Manager depicts the entire wireless network topology, updated on a user-configurable time basis. Access points appear under the agents that are monitoring their network segments. Mobile devices appear under the access points with which they are associated.

The most significant capability of Mobile Manager is its ability to define access-point profiles, essentially virtual access-point configurations stored in software. Multiple profiles can be defined as needed. You can also use Mobile Manager to define address-control lists that restrict entry into the network by MAC (Media Access Control) address. All address-control lists for a single site can be managed from one location, though admins will need to be know the per-access-point limitation in the number of address-control entries supported by vendors.

WEP (Wired Equivalent Privacy) keys can also be controlled using profiles, and firmware revisions can be applied automatically across the enterprise. Wavelink supports 40-bit WEP and is considering adding support for 128-bit keys. If you're looking for a management tool that lets you distribute WEP keys to client devices, this isn't it.

Another major capability revolves around monitoring. In addition to monitoring network traffic and access-point statistics, Mobile Manager provides configurable alert and alarm features. Statistical alerts can be defined for any data variable reported by an access point. Alarms can also be configured for critical events, including the appearance or disappearance of access points. Alarms can be forwarded to e-mail addresses or to network-management systems, like Hewlett-Packard Co. OpenView or Computer Associates' Unicenter. Finally, log files are created by each agent, and you can use the included log viewer for debugging purposes.

Still Some Work to Do

Mobile Manager is far from being a simple plug-and-play solution. I experienced a number of problems, particularly in attempting to manage Cisco access points.

I found the product to be more capable in managing Symbol access points than in managing Cisco Aironet products. Mobile Manager's heritage lies in a product called SNC24, which was designed to manage Symbol wireless network infrastructure in retail environments, some of which have thousands of access points across hundreds of locations. So Wavelink has a track record in large installations.

Mobile Manager uses Symbol's proprietary protocol to **detect access points** and standard SNMP to monitor and control access points. By configuring a "virtual access point" profile in Mobile Manager, I was easily able to push this configuration out to the Intel access point. I created a simple profile that included a new 802.11 ESSID (extended service set ID), a MAC address-control list and WEP security keys. Once I applied the changes, Mobile Manager reconfigured the access point and restarted it. Many configuration changes require access-point reboots, which will drop wireless users from the network, so take care with this rather powerful tool.

The problems I had managing my Aironet 340 and 350 were due to Wavelink's use of HTTP for those access-point configurations. Not only did this prove unreliable, but I also found that the system would not work on Cisco access points that were enabled with Web security. Wavelink plans to fix this before the final release and says it hopes a newly revised Cisco SNMP MIB will eliminate these problems.

Although all my problems were resolved, I never felt comfortable with the product's ability to manage even my rudimentary Cisco infrastructure. Reservations aside, Mobile Manager is a significant product that provides evidence of a maturing WLAN industry. For some organizations, deploying wireless infrastructure without a centralized management tool seems unthinkable. But Wavelink's pricing and try-before-you-buy policy make Mobile Manager worth a look.

Dave Molta is senior technology editor of Network Computing. He is also an assistant professor in the School of Information Studies at

Syracuse University and director of the Center for Emerging Network Technologies. Molta's experience includes 15 years in IT and network management. Send your comments on this article to him at dmolta@nwc.com.

VENDOR INFORMATION

Wavelink Mobile Manager, tiered pricing structure, contact vendor for details. Available: Now. Wavelink Corp., (425) 823-0111; fax (425) 823-0143. www.wavelink.com

<http://www.nwc.com/>

Copyright (copyright) 2001 CMP Media LLC

COPYRIGHT 2001 All rights reserved. No part of this information may be reproduced, republished or redistributed without the prior written consent of CMP Media, Inc.'

COMPANY NAMES: Cisco Systems Inc.--Products; Symbol Technologies Inc.--

Products; Wavelink Corp.--Products

GEOGRAPHIC CODES/NAMES: 1USA United States

DESCRIPTORS: Network management software; Software single product review

EVENT CODES/NAMES: 010 Forecasts, trends, outlooks;350 Product standards, safety, & recalls

PRODUCT/INDUSTRY NAMES: 7372611 (Network Management Software)

SIC CODES: 7372 Prepackaged software

NAICS CODES: 51121 Software Publishers

TICKER SYMBOLS: CSCO; SBL

TRADE NAMES: Wavelink Mobile Manager (Network management software)--
Evaluation

FILE SEGMENT: CD File 275

7/9/561 (Item 1 from file: 624)

DIALOG(R)File 624:McGraw-Hill Publications

(c) 2005 McGraw-Hill Co. Inc. All rts. reserv.

00877433

Computerizing patient education documents: Here's a way to clean out those files!

JERRY F. POTTS, MD

Postgraduate Medicine, Vol. 102, No. 2, Pg 39

August 1997

JOURNAL CODE: PGM

SECTION HEADING: DIGITAL DOC ISSN: 0032-5481

WORD COUNT: 1,333

TEXT:

In the March 1997 column, I outlined our clinic's attempt to move to an electronic medical record, which has been a slow and somewhat painful process. As a result of a grant from a local neighborhood group, we have also been concentrating on another project--to somehow computerize patient education handouts.

Problems getting handouts to patients

Many primary care clinics try to educate patients regarding various aspects of their disease. Certainly, informed patients are more able to recognize problems when they occur and to find suitable care when it is needed.

Unfortunately, during a busy clinic day, physicians often overlook or rush through the patient education aspect of care. That's why the most successful programs rely on some system for determining the need for and providing patient information that is structured into the clinic visit and does not depend entirely on the physician.

Many clinics have a formal discharge process that allows nurses or other

personnel (eg, social workers, diabetes educators, dietitians) to instruct patients as part of the clinic visit. In some cases, the physician makes a note of what is needed and someone else gives the educational material to the patient.

Problems keeping copies on hand

Finding the material can be another problem. Traditionally, patient education handouts are filed in a central location and handed to patients when they are discharged. Problems with this system include out-of-date material, unreadable photocopies, inadequate supplies of handouts on common topics, and ``creative'' filing systems that frustrate those trying to quickly locate the proper material for patients who typically want to get out the door.

Allowing a computer to take over the function is often the answer to these problems. Putting all patient education handouts in a simple database that can be used by all clinic personnel quickly does away with ``I can't read this,' ' ``We're out of that one,' ' and ``I wonder where that one disappeared to.' ' In addition, all the file space used previously is freed up, since handouts are ``stored'' in the computer and printed out only as needed.

Our plan to solve delivery problems

In our project, we attempted to move delivery of educational materials one step closer to the patient encounter. Clinic personnel were surveyed for their thoughts on the process, and we decided to let nurses select what handout was needed while they were still in the exam room with the patient. Nurses would have access to available handouts with a small handheld computing device; they'd select the one to be printed, and it would be ready for patients to pick up as they left the office.

We certainly did not have the needed expertise to put together such a complicated effort, so we approached a software firm in Minneapolis (Business Brothers, 612-853-3024) for their help in project development. We chose to work with Macintosh computers, since Macs and the handheld Newton 120 PDA (Personal Digital Assistant) produced the right combination of software and hardware for our project. After defining our needs (eg, number and types of devices, costs), developers put together software to run the system.

The hardware side of the system includes two Dayna ``wireless access points,' ' two LaserJet 4M printers, and a Mac 7200/100 (with an attached 600-dpi full-page scanner) wired together into a small Ethernet network. Each of the three PDAs has a Dayna wireless communication card in the PCMCIA slot. The Mac was set up as both the server for the system and the scanning workstation. The scanning software saves each scan as a postscript (.ps) file (200 to 300 K per page), which is stored with up to 10 key words in a 4th Dimension database application (available through ACI US, 800-881-3466, or on the Web at www.acius.com).

The Mac also works as a server for the wireless side of the system. Two wireless access points were placed far apart in the clinic for maximum coverage. An application runs continuously, **scanning** the wireless **access points** for any communication from the PDAs. Each PDA is assigned to one of the printers and is loaded with software that communicates via radio frequency technology to a wireless access point. Each of the wireless access points has an Ethernet connection that is wired to the same network that the Macintosh server is on.

Our plan in action

We scanned several hundred patient education documents in several languages (eg, Spanish, Hmong, Vietnamese) into the system and were ready to go. This is how the system works:

When a nurse wants a handout for a patient, he or she simply writes or types one of the key words for that handout into the PDA. (Handwriting recognition has improved significantly since it was introduced, so it is very simple to use, but there is also a small virtual keyboard that pops up on the screen, and keys can be tapped to ``type'' in key words.) The requested key word travels via radio frequency to the wireless access point, which hands off the request to the Ethernet connection and hence to the Mac. When the system locates the requested key word in the database, all matching document titles are sent back to the PDA. The nurse selects the desired document title, the request is sent back to the Mac, and the desired handout is printed at whichever printer the particular PDA is assigned to.

This may sound like a lot of communication, but all this back-and-forth occurs very quickly. We found that the total time from entering a key word to printing the finished document is less than 90 seconds.

Success with a price

The computerized patient handout system we came up with offers several advantages over a traditional paper filing system and even over other computer-storage systems. The most useful feature is its extreme portability. Because of the location of the wireless access points in the clinic, nurses can carry the PDAs into any exam room or work area and still access the database and print whatever is requested. We don't need to keep any paper copies, and new handouts can easily be added to the system. An important advantage is that each document receives a date of input when it is scanned, providing a useful reminder to review and update old material.

As with any new project, ours had many minor irritations. We were attempting to work with relatively new technologies in a new way. Most wireless applications only send information to a server, with no back-and-forth communication. The type of interaction we wanted made the software much more technical and tougher to put together. Add purchasing delays and personnel issues, and what started out to be a 6-week project took about 6 months. Being on the cutting edge can be painful!

Simpler ways to get handouts by computer

A quick and relatively painless way to access computer-based patient education information is through the World Wide Web. Several Web sites have extensive patient education libraries online (try www.vh.org/Patients/Patients.html or www.aafp.org/patientinfo). By having your browser up and running and pointed to one of these sites, you can do a quick key word search and bring the desired document up on the screen for printing. Disadvantages of such a system are that you are limited to topics that are already online and you cannot modify or add handouts.

Obtaining a disk or CD-ROM with patient education handouts ready to go is an even easier approach. For example, for about \$100, members of the American Academy of Family Physicians can buy a CD-ROM with English and Spanish text on nearly 200 problems typically seen in a family practice or primary care clinic through CMC Research Inc (503-242-2567; E-mail address, cmcresrch@aol.com; Web site, www.cmcresearch.com).

You may have a method of your own that works well or you may have no problems at all with your paper filing system, and that's great. It doesn't really matter how delivery is accomplished, just so it is. Patients clearly benefit from having a handout to refer to after they leave the clinic.

Copyright 1997 The McGraw-Hill Companies, Inc.

COMPANY NAMES: American Academy of Family Physicians ; Business Brothers ;
CMC Research Inc

7/9/680 (Item 1 from file: 696)
DIALOG(R) File 696:DIALOG Telecom. Newsletters
(c) 2005 The Dialog Corp. All rts. reserv.

00695445

CROWN CASTLE-METRICOM

WIRELESS TODAY

October 19, 1999 VOL: 3 ISSUE: 202 DOCUMENT TYPE: NEWSLETTER

PUBLISHER: PHILLIPS BUSINESS INFORMATION

LANGUAGE: ENGLISH

WORD COUNT: 94

RECORD TYPE: FULLTEXT

TEXT:

Houston-based Crown Castle International Corp. [TWRS] today entered a 10-year master license agreement with Metricom Inc. [MCOM] for up to 500 wireless data sites on Crown Castle's domestic communications towers.

Metricom is expected to co-locate wired access points, which are integral to its Ricochet high-speed wireless data network, in order to launch its 128 Kbps service next summer. Rental rates will be between \$1,500 per month and \$2,100 per month depending on the region where a site is located and the configuration of the site.

Crown Castle owns, operates and manages more than 7,000 wireless communication towers worldwide.

File 8: Ei Compendex(R) 1970-2005/May W3
(c) 2005 Elsevier Eng. Info. Inc.
File 35: Dissertation Abs Online 1861-2005/May
(c) 2005 ProQuest Info&Learning
File 65: Inside Conferences 1993-2005/May W4
(c) 2005 BLDSC all rts. reserv.
File 2: INSPEC 1969-2005/May W3
(c) 2005 Institution of Electrical Engineers
File 94: JICST-EPlus 1985-2005/Apr W1
(c) 2005 Japan Science and Tech Corp (JST)
File 6: NTIS 1964-2005/May W3
(c) 2005 NTIS, Intl Cpyrght All Rights Res
File 144: Pascal 1973-2005/May W3
(c) 2005 INIST/CNRS
File 434: SciSearch(R) Cited Ref Sci 1974-1989/Dec
(c) 1998 Inst for Sci Info
File 34: SciSearch(R) Cited Ref Sci 1990-2005/May W4
(c) 2005 Inst for Sci Info
File 99: Wilson Appl. Sci & Tech Abs 1983-2005/Apr
(c) 2005 The HW Wilson Co.
File 266: FEDRIP 2005/Jan
Comp & dist by NTIS, Intl Copyright All Rights Res
File 95: TEME-Technology & Management 1989-2005/Apr W3
(c) 2005 FIZ TECHNIK
File 256: TecInfoSource 82-2005/Apr
(c) 2005 Info.Sources Inc

Set	Items	Description
S1	180	(ACCESS() POINT? ?) (6N) (SCAN???? OR DETECT??? OR DISCOVER??? OR SWEEP??? OR SEARCH???)
S2	763	WIRELESS (3N) (ACCESS() POINT? ?)
S3	22	S1 AND S2
S4	18	RD (unique items)
S5	7	S4 NOT PY=2002:2005

5/5/1 (Item 1 from file: 256)
DIALOG(R)File 256:TecInfoSource
(c) 2005 Info.Sources Inc. All rts. reserv.

00153371 DOCUMENT TYPE: Review

PRODUCT NAMES: Distributed Wireless Solution (228245)

TITLE: SonicWall package aids WLAN security
AUTHOR: Garcia, Andrew
SOURCE: eWeek, v21 n30 p47(1) Jul 26, 2004
ISSN: 1530-6283
HOMEPAGE: <http://www.eweek.com>

RECORD TYPE: Review
REVIEW TYPE: Review
GRADE: B

Sonic Wall's Distributed Wireless Solution gets very good marks overall, with excellent marks for security, good marks for usability, capability, performance, and interoperability, and fair marks for manageability and scalability. The security advantages of wireless gateways are combined with the access point management features of wireless switch systems in one single platform that offers wireless LAN encryption, packet and application layer filtering, user authentication, access point management, and rogue detection. Testing was done on two 802.11 a/b/g compliant SonicPoint Access points and SonicWall's new Gigabit Ethernet-ready Pro 5060f firewall appliance running SonicOS Enhanced 2.5.0.2 firmware. The Pro5060f firewall appliance manages SonicPoint configuration profiles and pushes correct network settings and security settings to the access points. Packet and application layer filtering are done on all traffic by terminating all connections from wireless clients. A one-year subscription to SonicWall Intrusion Prevention Service is included in the purchase price. Hardware provisioning was uncomplicated during testing. Each SonicPoint has two configuration profiles (centrally managed and standalone mode; the standalone mode is the default when a governing appliance is not available, and standalone profiles have to be configured manually and one at a time with SonicWall's Secure HTTP interface).

PRICE: \$13,785

COMPANY NAME: SonicWALL Inc (509485)
SPECIAL FEATURE: Charts, Screen Layouts
DESCRIPTORS: Communications Interfaces; Internet Security; Wireless Networks
REVISION DATE: 20050300

5/5/2 (Item 2 from file: 256)
DIALOG(R)File 256:TecInfoSource
(c) 2005 Info.Sources Inc. All rts. reserv.

00151282 DOCUMENT TYPE: Review

PRODUCT NAMES: IPsonar 3.0 (216656)

TITLE: IPSonar rolls with net changes: Version 3.0 detects variety of...
AUTHOR: Sturdevant, Cameron
SOURCE: eWeek, v21 n10 p57(1) Mar 8, 2004
ISSN: 1530-6283
HOMEPAGE: <http://www.eweek.com>

RECORD TYPE: Review
REVIEW TYPE: Review
GRADE: B

Lumeta's IPsonar 3.0 tidily expands intrusion and **wireless access point detection** and can pinpoint possible information leaks across network borders. However, at \$18,000 per license for monitoring 5,000 IP addresses, IPsonar 3.0 is most suitable for high-value networks where IT management predicts considerable changes. IPsonar 3.0 ships with a 1U (1.75-inch) IPsonar Server that is also an IPsonar Sensor. Rated very good, IPsonar 3.0 gets excellent scores for capability and scalability, good scores for performance, interoperability, manageability, and security, and fair marks for usability. IPsonar 3.0 is recommended for IT managers planning to merge large networks, and managers who do security audits will also gain from IPsonar 3.0's large network and server mapping reports, which offered precise details regarding network layout. During testing, IPsonar 3.0 mis-identified a Cisco Systems' Aironet 1100 Series **wireless access point**. The problem was mistyped identification file. Response to the problem from Lumeta was fast, and IPsonar 3.0 had also successfully identified **wireless access points** from D-Link Systems and Buffalo Technology Group. IPsonar 3.0 also provides useful details describing individual devices, including which machines responded to FTP requests. Testers also were surprised that IPsonar 3.0 detected many, unexpected exposures of the network to the Internet. IPsonar 3.0 was very compelling in its ability to make sure the network is correctly limited to the subject lab, with no crossover to other networks.

PRICE: \$18000

COMPANY NAME: Lumeta Corp (755079)

SPECIAL FEATURE: Screen Layouts Charts

DESCRIPTORS: Computer Security; Intrusion Detection; Network Administration; Network Software; System Monitoring; WANS; Wireless Networks

REVISION DATE: 20040630

5/5/3 (Item 3 from file: 256)
DIALOG(R)File 256:TecInfoSource
(c) 2005 Info.Sources Inc. All rts. reserv.

00147913 DOCUMENT TYPE: Review

PRODUCT NAMES: RSA SecurID ACE/Server (796107); Remedy Help Desk (597295); PhpBrain (183687)

TITLE: Knowledge Base Boosts IT Reports
AUTHOR: Thurman, Mathias
SOURCE: Computerworld, v37 n34 p34(1) Aug 25, 2003
ISSN: 0010-4841
HOMEPAGE: <http://www.computerworld.com>

RECORD TYPE: Review
REVIEW TYPE: Product Analysis
GRADE: Product Analysis, No Rating

RSA Security's RSA SecurID and BMC Software/Remedy's Remedy are some of the components in an environment where, says a security manager, Sourceforge's PhpBrain open source tool proved to be useful as a repository for IT security support information. The IT security department is responsible for administration and maintenance of RSS Security ACE SecurID authentication servers, intrusion detection systems (IDSes), infrastructure, integrity-checking software, forensics tools, **wireless access point detection** and management software, and a data correlation environment. The enabling operating systems and their applications change often, and they are always being tweaked. Patches are continually added, and diagnostics are always being conducted. Taking manual notes is really not sufficient to create a problem resolution knowledgebase, but PhpBrain, which was

developed for a gaming project, is available as source code that can be used as a digital knowledgebase. The department uses PhpBrain, which is Web-ready, on a standard PC to allow easy information input, search, and retrieval. Another good tool is an incident-reporting program, which was developed internally by a programmer who wrote a back-end database to run on Microsoft SQL Server and coded the Web-based front end with Active Server Pages (ASP).

COMPANY NAME: RSA Security Inc (398047); Remedy Corp (516449); Open Source Developer Network (OSDN) (728446)
DESCRIPTORS: Computer Security; Intrusion Detection; Knowledge Exchanges; Network Administration; Network Software; Open Source; PHP; System Monitoring; Wireless Networks
REVISION DATE: 20031030

5/5/4 (Item 4 from file: 256)
DIALOG(R) File 256:TecInfoSource
(c) 2005 Info.Sources Inc. All rts. reserv.

00142647 DOCUMENT TYPE: Review

PRODUCT NAMES: 802.11b (845426); WEP (Wireless Equivalent Privacy) (844608)

TITLE: Wireless LAN attacks grow in sophistication
AUTHOR: Cox, John
SOURCE: Network World, v19 n43 p34(1) Oct 28, 2002
ISSN: 0887-7661
HOMEPAGE: <http://www.nwfusion.com>

RECORD TYPE: Review
REVIEW TYPE: Product Analysis
GRADE: Product Analysis, No Rating

IEEE's 802.11b's built-in Wireless Equivalent Privacy (WEP) security technology is a target for hackers, who are always updating freeware utilities and other programs, such as WEPcrack and Aircrack, which are attack applications. A spokesperson for a carrier software vendor says his company has to move to a virtual private network (VPN) for its wireless LAN, which would require each wireless users to authenticate, for instance, through a Remote Authentication Dial-In User Service server, and then would encrypt or scramble data moved between the wireless devices and the access point. However, a VPN can also be invaded in the wireless world via a man-in-the-middle attack, which permits intruders to obtain network information regarding access points or client adapters, including MAC addresses. The information can be used to impersonate already authenticated wireless LAN devices. Threats described include decoy access points, which can be countered with mutual authentication; access point maps, which can be foiled through security architecture, authentication, and encryption; invisible access points, which require security policies and intrusion detection; and automated low-level attacks on WEP keys, passwords, and addresses, which require IDS and access point configuration management. A spokesperson for Air Defense says users can find the exact longitude and latitude of an access point, then map directions to the site through MapQuest to get an aerial picture of the location.

COMPANY NAME: Vendor Independent (999999)
SPECIAL FEATURE: Tables
DESCRIPTORS: Encryption; Internet Security; LANs; Network Administration; Network Software; Privacy; System Monitoring; Wi-Fi; Wireless Networks
REVISION DATE: 20030330

5/5/5 (Item 5 from file: 256)

DIALOG(R)File 256:TecInfoSource
(c) 2005 Info.Sources Inc. All rts. reserv.

00139038 DOCUMENT TYPE: Review

PRODUCT NAMES: AirDefense (105155)

TITLE: Startup takes on WLAN security: AirDefense appliance includes...

AUTHOR: Fisher, Dennis

SOURCE: eWeek, p21(1) Jun 3, 2002

ISSN: 1530-6283

HOME PAGE: <http://www.eweek.com>

RECORD TYPE: Review

REVIEW TYPE: Product Analysis

GRADE: Product Analysis, No Rating

AirDefense's Linux-based AirDefense wireless LAN security appliance includes vulnerability assessment and other features that provide the same type of security for wireless networks that is available in the hard-wired world, say spokespeople for AirDefense. The AirDefense appliance returns results of the full vulnerability assessment to a Web-based console, which manages the network and displays data on alerts executed by the intrusion detection systems, a list of access points found on the network, and views of activity on each channel. AirDefense finds deployed access points, but also can unearth the ad hoc networks, or small groups of users with Wi-Fi cards who directly intercommunicate, rather than going through an access point, AirDefense's CEO and founder Jay Chaudhry points out that many users do not know that they such rogue networks operating inside their companies. The AirDefense appliance also monitors network traffic to make sure that access points have turned on Wireless Equivalent Privacy (WEP) encryption and are not broadcasting users' Service Set Identifiers (SSIDs). One venue used by attackers frequently against WLANs involves posing as an authorized user by stealing a SSID. In order to further guard against session hijacking, AirDefense developed one-of-a-kind fingerprints for all WLAN cards sold by leading vendors.

COMPANY NAME: AirDefense Inc (725391)

SPECIAL FEATURE: Screen Layouts Output Samples

DESCRIPTORS: Computer Security; Intrusion Detection; LANs; Linux; Network Administration; Network Software; System Monitoring; Wireless Networks

REVISION DATE: 20020830

5/5/6 (Item 6 from file: 256)

DIALOG(R)File 256:TecInfoSource

(c) 2005 Info.Sources Inc. All rts. reserv.

00138520 DOCUMENT TYPE: Review

PRODUCT NAMES: 802.11b (845426); 802.11a (845124); Connect Manager (101583)

TITLE: Wireless LAN Security Crackdown: Combine usage policies, detection...

AUTHOR: Brooks, Jason

SOURCE: eWeek, v19 n18 p45(3) May 6, 2002

ISSN: 1530-6283

HOME PAGE: <http://www.eweek.com>

RECORD TYPE: Review

REVIEW TYPE: Product Analysis

GRADE: Product Analysis, No Rating

IEEE's 802.11b and 802.11a and ReefEdge's ReefEdge Connect are highlighted

in a discussion of the deployment of usage policies and detection technologies that protect wireless LANs (WLANs) against security threats. The WLAN market is expected to ship 23.6 million units in 2005, up from 3.3 million in 2000. The cost of WLAN systems, including **wireless access points** based on 802.11b, has dropped precipitously. OEMs now offer laptops with integrated 802.11b radios. Intel also announced plans to include 802.11b support in its planned Banias mobile processor. To protect resources, however, IT managers will have to ensure that WLAN technology is constructed securely from the outset and will have to be sure that 'rogue' access points will not gain access to such resources. Companies can lower WLAN security exposure by positioning access points so their coverage area does not go outside the walls of a corporate campus. The occasional user, for instance, will not often think about how far the traffic generated by his or her rogue network will travel. The Service Set Identifier is generally the only security provided for such rogue access points, but where it is used, WLAN policies should be created and deployed. An anti-WLAN stance can be enforced with **sweeps** for rogue **access points** using such **wireless** sniffer products as AiroPeek NX, Snuffer Wireless 4.7, and Observer 8.1 Wireless Protocol Analyzer.

COMPANY NAME: Vendor Independent (999999); ReefEdge Inc (723533)
SPECIAL FEATURE: Charts
DESCRIPTORS: Communications Standards; Computer Security; LANs; Laptops;
Mobile Computing; Network Administration; Network Software; System
Monitoring; Wi-Fi; Wireless Networks
REVISION DATE: 20030330

5/5/7 (Item 7 from file: 256)
DIALOG(R)File 256:TecInfoSource
(c) 2005 Info.Sources Inc. All rts. reserv.

00137059 DOCUMENT TYPE: Review

PRODUCT NAMES: Harmony (085367); ORiNOCO Access Points (087739)

TITLE: Getting from a to b: Proxim Harmony bridges 802.11a and 802.11b...
AUTHOR: Address, Mandy
SOURCE: InfoWorld, v24 n5 p29(2) Feb 4, 2002
ISSN: 0199-6649
HOMEPAGE: <http://www.infoworld.com>

RECORD TYPE: Review
REVIEW TYPE: Review
GRADE: B

Proxim's Harmony and Agere Systems' Agere Orinoco AS-2000 are products that allow companies to secure WLAN systems. Companies need such solutions to support their 802.11a and 802.11b networks, and Proxim Harmony allows them to link 802.11a, 802.11b, and OpenAir wireless devices for interoperation on the same network. Users can therefore communicate, irrespective of the devices in use, and all devices are centrally manageable from a Web interface. Proxim Harmony is a user-friendly, economical, wireless networking solution that supports roaming across subnets. The central component of Harmony is the **Access Point Controller**, a standalone device, that automatically **discovers all wireless access points** on the network and allows central administration via a Web interface. Agere Orinoco AS-2000 is a very well designed and effective security solution that provides authentication, authorization, and accounting for Wi-Fi connections so that companies can make sure that only known, authorized users gain access to their networks. Access points include RADIUS (Remote Authentication Dial-In User Service) servers for user authentication before users can sign on to the wireless network. AS-2000 also exchanges encryption keys for each session and each user, which improves Wireless Equivalent Privacy's (WEP's) security. The AS Manager component, a Java

application, manages configuration and monitoring, providing extensive ease of use and also streamlines access point administration considerably.

COMPANY NAME: Proxim Inc (547816)

SPECIAL FEATURE: Charts

DESCRIPTORS: Computer Security; LANs; Network Administration; Network Software; Wireless Networks

REVISION DATE: 20030730